THE SCHOOLS OF KING EDWARD VI IN BIRMINGHAM

In pursuit of educational excellence for all

KING EDWARD VI ACADEMY TRUST BIRMINGHAM

Online Safety Policy	
Responsible Board/Committee	Academy Trust Board Foundation Board
Policy Type	Hybrid Policy
Policy Owner	Foundation Leader in Education – Safeguarding and Wellbeing
Statutory	Yes
Publish Online	Yes
Last Review Date	June 2024
Review Cycle	Annual This policy will not expire but will be reviewed as per its designated cycle. This policy remains effective whilst the review is taking place and will only become non-applicable once the updated version has been approved.
Next Review Date	August 2025
Version	3.1

School	King Edward VI Handsworth Wood Girls' Academy
School Policy Owner	S Dennis

LGB Approval Date	September 2024

Contents

1. Introduction

Purpose
The purpose of this policy is to set out a framework outlining the King Edward VI Foundation and Academy Trust's approach to safeguarding and child protection in relation to online safety.

Definitions
The King Edward VI Foundation (the 'Foundation Charity') (registration no. 529051) charity, comprises two Independent Schools and the Foundation Office. The King Edward VI Academy Trust Birmingham (the 'Academy Trust') (registration no. 10654935) incorporates the Academies. (The Foundation Charity and the Academy Trust are collectively known as the 'Foundation'.)

Commitment
The Foundation is committed to safeguarding and promoting the welfare of all its pupils by delivering an effective approach to online safety, that empowers the Foundation to protect and educate the whole school community in its conduct and use of all technology.

We believe that:

- All young people have the right to be protected from harm, abuse and exploitation, including online.
- That every young person has the right to be safe and to feel safe in school.
- All young people should respect and support each other, both off- and online.
- By having clear systems and robust processes in place, staff can be proactive in identifying, intervening and escalating an incident where appropriate.
- All staff and visitors have an important role to play in safeguarding young people and protecting them from abuse and exploitation both off- and online.

King Edward VI Handsworth Wood Girls' Academy will follow Keeping Children Safe in Education 2024 in reference to:

- Safeguarding information for all staff.
- What school staff should know and do.
- A child centred and coordinated approach to safeguarding.

This policy cannot be separated from our general ethos and safeguarding culture within school which ensures that students:

- are treated with respect and dignity.
- are taught to treat each other with respect.
- feel safe.
- have a voice and are listened to, ensuring that our approach to safeguarding is child-centred, always considering the best interests of the child.

Safeguarding and promoting the welfare of children is everyone's responsibility. Everyone who encounters young people, and their families has a role to play to fulfil this responsibility effectively, including identifying concerns, sharing information and taking prompt action.

Diversity and Equality Mission Statement

We believe that all members of our community are entitled to be treated fairly and equally regardless of their race, ethnicity, religion, gender, sex, sexuality or disability. Our purpose is to challenge discrimination in all its forms so that our students can achieve educational excellence.

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.

2. Legislation and Guidance

In recent times, government and regulatory bodies have intensified their efforts to establish guidelines which balance the benefits of digital connectivity with the need to shield young people from potential harm and privacy breaches. In the UK, the Department for Education (DfE) has introduced and continues to upgrade its statutory online safeguarding requirements for schools. For example, UK schools are required to have ‘appropriate filters and monitoring systems in place and regularly review their effectiveness’.

This policy is therefore based on the following:

- HM Government Statutory Guidance: Working Together to Safeguard Children
- DfE Statutory Guidance: Keeping Children Safe in Education
- DfE Meeting digital and technology standards in schools and colleges
- UK Safer Internet Centre: appropriate filtering and monitoring. A guide for education settings.
- The government guide to the new Online Safety Bill
- DfE guidance: mobile phones in schools
- Government guidance on teaching online safety in schools
- Government guidance on preventing and tackling bullying
- Government guidance on the powers schools have in searching, screening and confiscation .
- Unicef policy guidance on AI for children
- World Economic Forum: artificial intelligence for children toolkit

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.

2.1 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 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.

While complying with data protection legislation is important and will always be considered, the safeguarding of students is our main priority – concerns around data protection should not prevent a safeguarding disclosure being investigated.

2.2 Children's data

The Child Safeguarding and Immersive Technologies report commissioned by the NSPCC notes that how children's data is used in Virtual Reality (VR) is a key issue in terms of safeguarding. Data privacy can be a double-edged sword. It can help to encourage child safeguarding and reduce the risk of abuse and exploitation, particularly the risks of an offender accessing a child's location and contact details; or the risk of an offender accessing images of a known child to use that to create a child model for sexual gratification. However, data encryption can also pose risks: protecting offenders' identities and hiding abusive content.

The above report also noted that an important part of a platform's objectives is to maximise data collection: collecting information about users, such as where users go, what they do, who they speak to and what they purchase. Many technology companies' investment models assume that user engagement = valuable user data extraction. In direct opposition to this model, the Information Commissioner's Office (ICO) recently released the Children's Code, insisting that providers "cannot collect more data than you need to provide the elements of a service the child actually wants to use". Any excessive collection of data could have significant implications for children who use VR and AR, potentially exposing them to privacy risks and the misuse of their personal information. As immersive environments become more realistic and engaging, the data collected from children's interactions can reveal their habits, preferences, and even emotional states. This level of personal data could potentially be exploited.

Privacy violations can also cause significant detriment to a child, including through harmful targeted advertising, for example, or data sales. Privacy violations could also be more direct: an offender hacking into a parent's online photograph storage and using that visual material to build a realistic replica of the child via AI tools referenced above.

2.2 Filtering and monitoring

Our school uses Smoothwall to monitor online activity connected to school devices. In 2023 globally Smoothwall spotted a child at potential serious risk every 56 seconds and every 5 minutes they found a potentially vulnerable child. In our school when a concern is noted by Smoothwall, the Designated Safeguarding Lead or Deputies are notified immediately, and action is taken. In cases where there is reference to suicide, Ripple interjects (see appendix 5) with signposting to support and advice services.

3. Roles and responsibilities

Emerging technologies bring both opportunities and risks, particularly in relation to child safety. Offenders seek out online spaces which children use, where they initiate contact, groom and abuse them, and seek to meet them offline, so it is everyone's responsibility to develop their understanding of the ever changing digital and technology landscape and the potential risks caused to children.

3.1 The Trustee Board and-School Governing Body

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

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, our governing body will do all that it reasonably can to limit children's exposure to online safety risks. As part of this process, they will ensure our schools have appropriate filtering and monitoring systems in place and will regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Our governing body will consider the number of and age range of our pupils, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

The School Governing Body will review case studies and data in relation to online safety incidents provided by the Designated Safeguarding Lead (DSL) as part of the termly report on safeguarding in the school.

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 1);
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and exploitation 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 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.

3.3 **The Designated Safeguarding Lead (DSL)**

[Schools may need to adapt the below according to job descriptions, however, schools should ensure all these responsibilities are covered.]

Details of the school's Designated Safeguarding Lead (DSL) and any deputies are set out in each school's Safeguarding and Child Protection Policy.

The DSL should be appropriately trained in digital safety issues (including understanding the filtering and monitoring systems and processes in place).

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 concerns, discussions and decisions, including the rationale for those decisions are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Managing all online safety issues and incidents in line with the school Safeguarding and Child Protection, Anti-bullying and No Platform for Extremism policies.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- Ensuring any instances related to online radicalisation are logged, including instances where referrals were or were not made to another agency such as the Local Authority or the Prevent program (see the school's No Platform for Extremism Policy for further information on this topic).
- Updating and delivering staff training on online safety and preventative digital safeguarding measures (appendix 3 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 School 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.

3.4 **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, without unreasonably impacting teaching and learning.
- Ensuring that any online safety incidents are logged (see appendix 4) 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
- Working closely with the Designated Safeguarding Lead (DSL) and other staff to address any online safety issues or incidents.

This list is not intended to be exhaustive.

3.5 The School Community

Pupils, staff and parent/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 always representing the Schools of King Edward VI community and must act appropriately.

3.6 All Staff and Volunteers

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 (appendix 2), 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 (see appendix 4) 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 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

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

This list is not intended to be exhaustive.

Staff need to acknowledge **the silencing effect** as a phenomenon of self-censorship that occurs when individuals, particularly girls and minority groups, face online harassment, trolling or intimidation. It is imperative that staff learn to recognise the behaviour associated with pupil experiences and identify ways to intervene early to minimise negative impacts.

Staff must be able to understand that the digital habits, behaviour, and risks/vulnerabilities experienced by children can often be spotted through their digital behaviour. By monitoring online behaviour such as searches and interactions, Smoothwall allows staff in school to identify patterns and behaviour that may negatively impact wellbeing. Staff also need to be able to provide opportunities for pupils to report online conflict to prevent the escalation of social, emotional, psychological, or physical harm.

All staff, governors and volunteers should receive appropriate online safety training which amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

As part of their training, staff should be made aware of the Online Safety Act and any changes that will affect the practice of professionals working with children. The Act places the onus on technology companies to keep children safe on their services and platforms. Social media companies will have to provide adults and children with clear, accessible and easy-to-use ways to report problems and make complaints online if harms arise so, if a site is falling short of the required standards, it should be easy to raise concerns with the platform.

If staff/parents/carers have ongoing concerns about a platform, they can make a complaint to Ofcom. While Ofcom cannot respond to individual complaints, this information can help them to assess which services are complying with the regulation.

The Act also introduces new criminal offences, including:

- an intimate image abuse offence, which makes it a crime to share an intimate image of someone without their consent;
- a 'cyberflashing' offence, which criminalises sending an explicit image for the purpose of sexual gratification or to cause the recipient humiliation, alarm or distress.

3.7 Parents/ Carers

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. In 2023 research found that more teenagers were using social media platforms for their news consumption, rather than traditional media. This has opened the floodgates for the influencers they follow, who may have skewed opinions, credibility, or evidence for their beliefs, to act as educators for children on complex world events. Instagram is now the most popular news source among younger people – used by 29% of teenagers in 2022 – with TikTok and YouTube close behind. It is important that parents talk to their children about potential misinformation or fake news in relation to what they read and hear online.

The nature of immersive technologies, such as virtual reality (VR) headsets, can make it difficult for parents/carers to monitor what their children are experiencing in virtual environments. Unlike with the 2D internet, caregivers cannot simply look over their child's shoulder and view their computer screen. Instead, the child is immersed in a virtual world only visible to them. It is important, therefore, that parents understand that VR is more than 'just a game' and it does come with risks. Commissioned NSPCC research found that while exposure to inappropriate content was a concern for three quarters of parents when they were asked to reflect on children's online use, fewer than half felt that this was a concern when asked to reflect on children's engagement with the metaverse, virtual reality or augmented reality. It is important, therefore, for parents to consider close supervision of children engaging with VR.

Appropriate home use of the Internet by children can of course be educationally beneficial and can make a useful contribution to home and schoolwork. It too should be supervised, and parents/carers should be aware that they are responsible for their children's use of Internet resources at home and the outcome of any inappropriate usage that impacts on them or their peers once in school.

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 via telephone or email.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

6

4.8 Visitors and members of the community

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.

4. 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, Islamophobia, faith and hate crime, radicalisation and extremism. Children may feel that they should 'not make a big deal' out of the harms that happen to them in VR. They may fear they will not be taken seriously, or an adult will not understand as it is 'not real'. This could lead to a reduced likelihood of disclosing incidents to parents, carers, educators, platform moderators, or law enforcement, so we need to educate our pupils to understand that abuse is abuse whether offline or online.
- **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 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 scams. In 2022, UK consumers lost approximately 1.2 billion pounds in online scams, and young people went from being collateral damage in scams to being specific targets. Many fell victim to online scams, including phishing attempts, buying and selling scams through spoofing or fraudulent websites, and deceptive online strangers targeting young people with sextortion-style scams, leading to financial loss and even identity theft. If you feel pupils or staff are at risk, please report it to the Anti-Phishing Working Group.

All secondary schools must teach Relationships and Sex Education and Health Education and PSHE (personal, social, health and economic). Most of PSHE education became statutory in September 2020 under the Children and Social Work Act. The Act introduced compulsory Relationships and Sex Education in secondary schools. Health Education (both mental and physical) became statutory from key stages 1 to 4.

Pupils will be taught about online safety as part of the curriculum.
[The text below is taken from the National Curriculum computing programmes of study. Schools that do not follow the National Curriculum should adapt this section to include details of how online safety forms part of their own 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.

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, exploitation 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.

5. 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 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 will also be covered during parents' / carers' evenings and parent drop-in sessions.

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 harmful content - UK Safer Internet Centre - a national reporting centre designed to assist anyone reporting harmful content online.
- Report a concern to Child Exploitation and Online Protection Safety Centre (CEOP) that a child is being groomed online or sexually exploited: parent/carer guide to reporting an incident.

6. Cyber-Bullying

6.1 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. (See also the school Behaviour and Anti-bullying policies.) 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.

The rise of deepfake technology now means cyberbullying can become more personalised, targeted and hyperrealistic. It can lead to serious emotional distress, feelings of shame and resentment, and damage to the self-esteem of children. For some it can even lead to self-harm and suicide.

6.2 **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.

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, 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, 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.

Class teachers/form teachers 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.

All 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. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to 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.

6.3 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) with pupil consent to search for examine, and, if necessary, delete or supervise the deletion of 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 e.g. the data, image or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. These powers are compatible with Article 8 of the European Convention on Human Rights.

Members of staff cannot, however, search for/view material that is deemed to be sexually explicit/inappropriate. If there is concern about material on a phone during a search, the local police will be notified, and the electronic device will be searched by them.

If inappropriate material is found on the device a Pastoral Lead or Senior Leader can: retain the device as evidence (of a criminal offence or a breach of school discipline or whether the material is of such seriousness that it requires the involvement of the police); inform parents so they can report a concern to the police/service provider; or support the child to use 'Report Remove' or refer to Child Exploitation and Online Protection (CEOP).

Parents/carers do not need to be informed before a search takes place but would normally be contacted afterwards, regardless of the outcome of the search.

The Governing Body and the Headteacher expect staff conducting searches to act with discretion and within the bounds of the law. The Headteacher/member(s) of the Leadership Team would be kept informed.

More detailed advice on confiscation and what must be done with prohibited items found as a result of a search is provided in Searching, screening and confiscation at school - GOV.UK

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

7. Acceptable Use of the 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 appendices 1 and 2.

03

8. 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 sexually 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.

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.

Mobile phones should be 'off and away' at all times, any phone seen or heard will be confiscated, this includes phones on display and in shirt pockets etc.

- **The first instance that a mobile phone is heard or seen, it will be confiscated and put in the school safe in a named envelope until the end of the week, parents will need to come in and collect it.**
- Should there **be a second occurrence, a telephone call will be made home with the requirement for a parent/carer to collect the mobile phone and the phone could be kept for a longer period of time.**

9. 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 *2*.]

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. If they receive inappropriate contact or content, including threats or defamation, they should report to their Line Manager immediately.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

10.1 Misuse

Where a pupil misuses the school's technology and digital systems or internet, we will follow the procedures set out in the Behaviour, Attitides and Rewards 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.

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded.
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and, making, supplying or obtaining malware (malicious software) such as viruses, spyware ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the Designated Safeguarding Lead (or deputies), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK

10.2 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, many 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 www.saferinternet.org.uk 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.

11. 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, e-bulletins and staff meetings).

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

- technology and digital systems are a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse and exploitation.
- 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; and
    - sharing of abusive images and pornography, to those who do not 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 and exploitation;
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up; and
- 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 about 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.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

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

A review of our filtering and monitoring provision will be completed at least annually.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Safe use of artificially intelligent tools policy
- Behaviour, Attituddes and Rewards policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Code of Conduct

Appendix 1: ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS / CARERS)

ICT Acceptable Use Agreement: Students

- I will only use the academy's ICT systems, including the internet, email, digital video, online services and mobile technologies for academy purposes.
- I will not download or install software on devices provided by the academy.
- I will only log on to the academy network, other systems and resources with my own user name and password.
- I will follow the academy's ICT security system and not reveal my passwords to anyone and change them as required.
- I will only use my academy email address for online communications with staff/students and any other third parties I am working with for academy purposes (such as for work experience or an academy project).
- I will make sure that all ICT communications with students, staff or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone I have communicated with online and will report such a request to a member of staff, or a responsible adult at home, immediately.
- I am aware that when I take images of students and/or staff, that I must only store and use these for academy purposes in line with the academy's data protection policy and must never distribute these outside the academy network without the permission of all parties involved. This includes academy breaks and all occasions when I am in academy uniform (onsite and offsite) or when otherwise representing the academy.
- I will ensure that my online activity, both in academy and outside academy, will not cause my academy, the staff, students or others distress or bring the academy community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the academy approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the academy community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to relevant academy staff.
- I understand that these rules are designed to keep me safe and that if they are not followed, academy sanctions will be applied and my parent/carer will be contacted.
- I will not sign up to online services that I am not old enough to use.

Device Loan Agreement Form

Student Name:_____

Date: _____

A King Edward VI Handsworth Wood Girls' Academy device is being loaned to the borrower for academic purposes. It is my responsibility to care for the equipment and ensure it is maintained in a safe environment. If the device is lost, stolen or damaged, parents/guardians/students should immediately inform the academy ICT Network manager.

The device, device charger, charger cord and carrying case are the property of King Edward VI Handsworth Wood Girls' Academy and is herewith being loaned to the student for educational purposes only for the academic years whilst studying at the academy. Students may not deface or destroy this property in any way. Inappropriate material on the machine may result in the student losing their right to use this computer and face disciplinary action as stated in the academy behaviour policy. The equipment will be returned to the school on a date to be requested or sooner if the student leaves prior to the end of the academy academic year. Students who do not return the computer and related materials when requested may be subject to criminal prosecution or civil liability. A late fee may be charged if the device is not returned to the academy on the required check-in date.

If the device equipment is lost, stolen or damaged while in the borrower's possession, the borrower is responsible for the replacement or repair thereof and the academy against any claim occurring during or resulting from borrower's possession or use of the academy property, including, but not limited to any claim for infringement or violation of applicable trademarks and copyrights attributable to the borrower's use of the device. The borrower may use device equipment only for non-academic purposes, in accordance with the academy's IT User Declaration (which I will also be required to sign).

Any included software may be used only in accordance with the applicable license and it is the borrower's responsibility to be familiar with and to comply with the provisions of such license. Borrower may not install or utilize any software in connection with the borrower's use of the device equipment other than software owned by the academy and made available in accordance with this receipt and agreement and the borrower agrees not to make any unauthorized use of or modifications of such software.

The academy is not responsible for any computer or electronic viruses that may be transferred to or from the device or other data storage medium and the borrower agrees to make their best efforts to avoid the device being damaged or rendered inoperable by any such electronic virus while in their possession. By signing below, borrower and borrower's parent/guardian acknowledge and agree to the terms of use as spelled out in this Device Loan Agreement Form.

Parent's Signature: _____

Print Name: _____
Date: _____

Student Signature: _____
Print Name: _____
Date: _____

King Edward VI Handsworth Wood Girls' Academy
Device Loan Agreement Summary

Student Responsibilities
Your device is an important learning tool and is for educational purposes only. In order to take your device home each day, you must be willing to accept the following responsibilities:

 I know this computer is on loan to me. All academy policies, procedures and applicable laws must be followed. I understand that any violation could result in loss of the device for my use or disciplinary action as stated in the academy behaviour policy.
 I will treat the device with care and will be responsible in using the device.
 I will not loan the device to others, it will stay in my possession at all times.
 I will not load or delete any software from the device and I will comply with all copyright laws.
 I will not remove or alter the device label or the ID inventory number.
 I will not give personal information when using the Internet.
 I will not attempt to make any repairs to the device.

Parent Responsibilities
Your child has been issued a device to improve and personalise her education whilst studying at the academy. It is essential that the following guidelines be followed to ensure the safe, efficient, and ethical operation of your child's device.

 I will discuss academy policies and expectations regarding the use of the Internet and will supervise my child's use of the device at home.
 I will not attempt to make any repairs to the device.
 I will report to the academy any problems with the device.
 I will not load or delete any software from the device and I will comply with all copyright laws.
 I know that if my child comes to the academy without her device I may be called to bring it to the academy.

Student user IT Declaration

Handsworth Wood Girls' Academy - IT User Declaration

1.0 Purpose

This statement has been established to:

1.1 Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for use by Students.

1.2 Encourage users to understand their own responsibility for protecting the school's assets.
6000006
2.0 Audience

2.1 These principles apply to: Students using academy provided ICT equipment connected locally or remotely to the network of the academy. Throughout this policy, the word 'user' will be used collectively to refer to all such individuals or groups.

3.0 Mobile Devices (including iPad, iPhone, Tablet, Laptop and any other type of mobile device)

3.1 The use of mobile devices for ICT, introduces security implications including:

- Loss or theft of the mobile device
- Loss of business information on the mobile device
- Unauthorised network access
- Data integrity

3.2 Users therefore have a duty of care whilst using such devices to ensure that they are used for their intended purpose, without creating risks, by understanding the way the mobile devices should be used.

3.3 All academy supplied devices i.e. iPhone, Tablet, iPad, Laptop are the property of the academy and so it has the right to audit and monitor the device, similar to any other electronic device.

3.4 Users must take reasonable care to protect the device from loss or theft. The device should be locked away while not in use and adequate home insurance should be obtained to cover the cost of a like for like replacement in the event of theft. The device should not be left in your vehicle unattended.

3.5 Users must immediately inform the IT Technicians when the device is damaged, stolen or lost.

4.0 Use of the Academy Network, Emails and Firefly

4.1 Users understand and accept that they are responsible for reading other ICT related academy policies (Including E-Safety Policy).

4.2 The holder of an academy computer account or computer system connected to the academy network is responsible for the actions associated with the computer account or computer system.

4.3 Users must respect the rights, privacy and property of others.

4.4 Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared and a strong password must be used:

A strong password:

- Are at least eight characters in long.

- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four categories:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers/Symbols	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, #, $.....

4.5 Passwords must not be disclosed to anyone. Temporary passwords provided by IT staff to users must be changed immediately following a successful login.

4.6 Passwords will automatically run out after 90 days and will prompt users to change.

5.0 Data Protection

5.1 Users of the academy network and devices belonging to the academy must adhere to the Data Protection Act (1998) at all times.

5.2 Network and system passwords must not be stored on mobile devices or written down.

5.3 Users must take appropriate measures to protect against the accidental loss, damage or theft of academy information held on mobile devices, especially if that information relates to personal information.

5.4 If a devices logged onto the network is left unattended, it should be locked to require the user password in order to gain access to the device.

5.5 Portable storage devices (including memory sticks/USB stick, external hard drives, DVD's, CD's or any other portable media) must not be used on the academy network.

ICT User Declaration

I hereby acknowledge receipt of my ICT User Declaration and accept that it is my responsibility to read and comply with all policies.

Please Print:

Surname: _____ Forename: _____

Signature: _____ Date: _____

Appendix 2: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

ICT Acceptable Use Agreement: Staff, Governors, Volunteers and Visitors

- I will only use the academy's ICT systems, including the internet, email, digital video, online services and mobile technologies for academy purposes.
- I will only log on to the academy network, other systems and resources with my own user name and password.
- I will follow the academy's ICT security system and not reveal my passwords to anyone and change them as required.
- I will only use my academy email address for online communications with staff/students and any other third parties I am working with for academy purposes (such as for work experience or an academy project).
- I will make sure that all ICT communications with students, staff or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately.
- I am aware that when I take images of students and/or staff, that I must only store and use these for academy purposes in line with the academy's data protection policy and must never distribute these outside the academy network without the permission of all parties involved.
- I will ensure that my online activity, both in academy and outside academy, will not cause my academy, the staff, students or others distress or bring the academy community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the academy approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the academy community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that these rules are designed to safeguard the academy, students and myself and that if they are not followed, academy disciplinary procedures will be applied.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to relevant academy staff.
- I understand that removable media is not to be used on the academy network

IT User Declaration

Handsworth Wood Girls' Academy - IT User Declaration

1.0 Purpose

This statement has been established to:

1.1 Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for use by teachers, professionals and support staff.

1.2 Encourage users to understand their own responsibility for protecting the school's assets.

2.0 Audience

2.1 These principles apply to: teachers, support staff and all others using academy provided ICT equipment connected locally or remotely to the network of the academy. Throughout this policy, the word 'user' will be used collectively to refer to all such individuals or groups.

3.0 Mobile Devices (including iPad, iPhone, Tablet, Laptop and any other type of mobile device)

3.1 The use of mobile devices for ICT, introduces security implications including:

- Loss or theft of the mobile device
- Loss of business information on the mobile device
- Unauthorised network access
- Data integrity

3.2 Users therefore have a duty of care whilst using such devices to ensure that they are used for their intended purpose, without creating risks, by understanding the way the mobile devices should be used.

3.3 All academy supplied devices i.e. iPhone, Tablet, iPad, Laptop are the property of the academy and so it has the right to audit and monitor the device, similar to any other electronic device.

3.4 Users must take reasonable care to protect the device from loss or theft. The device should be locked away while not in use and adequate home insurance should be obtained to cover the cost of a like for like replacement in the event of theft. The device should not be left in your vehicle unattended.

3.5 Users must immediately inform the IT Technicians and Finance Team when the device is damaged, stolen or lost. Users will be asked to replace some items. This decision will be reviewed case by case. As Apple Pencils are part of a lease any staff member losing this item will be responsible for its replacement irrespective of circumstance..

4.0 Use of the Academy Network, Emails and Firefly

4.1 Users understand and accept that they are responsible for reading other ICT related academy policies (Including E-Safety Policy) and the Staff Handbook.

4.2 The holder of an academy computer account or computer system connected to the academy network is responsible for the actions associated with the computer account or computer system.

4.3 Users must respect the rights, privacy and property of others.

4.4 Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared and a strong password must be used:

A strong password:

- Are at least eight characters in long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.

- Is significantly different from previous passwords.
- Contains characters from each of the following four categories:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers/Symbols	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, #, $.....

4.5 Passwords must not be disclosed to anyone. Temporary passwords provided by IT staff to users must be changed immediately following a successful login.

4.6 Passwords will automatically run out after 90 days and will prompt users to change.

5.0 Data Protection

5.1 Users of the academy network and devices belonging to the academy must adhere to the Data Protection Act (1998) at all times.

5.2 Network and system passwords must not be stored on mobile devices or written down.

5.3 Users must take appropriate measures to protect against the accidental loss, damage or theft of academy information held on mobile devices, especially if that information relates to personal information.

5.4 If a device logged onto the network is left unattended, it should be locked to require the user password in order to gain access to the device.

5.5 Portable storage devices (including memory sticks/USB stick, external hard drives, DVD's, CD's or any other portable media) must not be used on the academy network, or to store any data relating to the academy, staff or students without agreed permission from the Headteacher. If permission is granted for a specific reason, an encrypted media device must be used.

ICT User Declaration

I hereby acknowledge receipt of my ICT User Declaration and accept that it is my responsibility to read and comply with all policies.

Please Print:

Surname: _____ Forename: _____

Signature: _____ Date: _____

Appendix 3 – Student expectations – Chromebooks

KING EDWARD VI
HANDSWORTH WOOD
GIRLS' ACADEMY

STUDENT DEVICE USE EXPECTATIONS

- My Chromebook will never be left unattended in any unsupervised area.
- I will not deface my Chromebook
- I will not lend or share my Chromebook with other pupils unless expressly asked to do so by a teacher in a classroom situation.
- I will not let friends and family use my Chromebook.
- If I leave my Chromebook at home I am responsible for getting any assignments or coursework completed as if I had my Chromebook present.
- I will bring my Chromebook to school each day in a fully charged condition.
- I will always turn off/lock and secure my Chromebook after I am done working to protect my work and information.
- I will use my Chromebook in a responsible and ethical manner
- I will not use another student's Chromebook without permission.
- I will make sure my Chromebook is put away unless I am asked to use it in lessons.
- I will only use an app that a teacher has asked me to use in lesson.
- I will not message other students on my Chromebook in lesson unless asked to by a teacher.
- I will not play games on my Chromebook in a lesson.
- I will not take photos of other students without their permission.
- I will stay on task on my Chromebook.

Appendix 4 – Student expectations – Ipads

KING EDWARD VI
HANDSWORTH WOOD
GIRLS' ACADEMY

STUDENT DEVICE USE EXPECTATIONS

- My iPad will never be left unattended in any unsupervised area.
- I will make sure a protective case is used with the iPad at all times.
- I will not lend or share my iPad with other pupils unless expressly asked to do so by a teacher in a classroom situation.
- I will not let friends and family use my iPad.
- If I leave my iPad at home I am responsible for getting any assignments or coursework completed as if I had my iPad present.
- I will bring my iPads to school each day in a fully charged condition.
- I will always turn off/lock and secure my iPad after I am done working to protect my work and information.
- I will use my iPad in a responsible and ethical manner
- I will not use another student's iPad without permission.
- I will make sure my iPad is put away unless I am asked to use it in lessons.
- I will only use an app that a teacher has asked me to use in lesson.
- I will not message other students on my iPad in lesson unless asked to by a teacher.
- I will not play games on my iPad in a lesson.
- I will not take photos of other students without their permission.
- I will stay on task on my iPad.

Appendix 5: 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-support on sexting.

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
Whether you are a digital expert or are 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.

NSPCC: what is the metaverse? Overview of risks and advice for parents

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.

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

Child Safety Digital: A practical guide for parents and carers whose children are using social media.

Snapchat digital safety.

What is Instagram and how is it used?

What is Snapchat and how is it used and Snapchat support - submit a request.

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

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.

Connect Safely Guides to media literacy, security, safety, wellness and fake news.

Teachers or parents / carers can sign up to the safety-adviser newsletter.

Staff

Ripple is an online interceptive tool designed to ensure more help and support is provided to individuals conducting searches related to self-harm or suicide. Created by Alice Hendy, who tragically lost her brother, Josh, to suicide in November 2020, Ripple focuses on proactive intervention, bridging the gap between individuals in crisis and the help they require. Here's how Ripple works:

1. **Silent Guardian**: When installed on a network or device, the Ripple tool discreetly monitors user searches without gathering personally identifiable information or interfering with existing technology. It operates silently in the background.
2. **Activation**: Ripple maintains an extensive database of keywords and phrases related to suicide and self-harm. If an individual searches for any of these flagged terms, the tool identifies it and initiates the intervention process.
3. **Intervention**: A calm pop-up message appears on the user's device, accompanied by a message of hope. The person in crisis is then provided with a selection of 24/7 helplines and mental health resources that they can access immediately and in the longer term.

The aim of Ripple is to shield users from accessing harmful content online and provide a lifeline for those in a mental health crisis. Visit the Ripple website for additional information and resources

Smoothwall Online Safety Hub: A dedicated resource to help schools and parents have meaningful conversations with children about their digital safety and wellbeing.

Smoothwall Digital Wellbeing: State of the Nation Report 2024. A report on student digital wellbeing, online risks, blindspots and school strategies for thriving in the digital era.

Project Evolve: shaping a better online life for all.

South West Grid for Learning (SWGfL) a charity dedicated to empowering the safe and secure use of technology through innovative services, tools, content and policy, nationally and globally.

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

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.

Safeguarding Essentials every teacher needs to know about e-safety.

Internet study looks at several vulnerable groups to ascertain differences of experiences and vulnerabilities.

POSH Supporting you to deliver education and raise awareness of digital child exploitation and abuse.

Brook publications' research project looks at how young people use technology in developing romantic relationships and surviving break ups.

NEN Education Network Leading educational support for helping you stay safe digitally.
Educate Against Hate website gives teachers, parents and school leaders practical advice and information on protecting children from extremism and radicalisation.

This briefing note is aimed at head teachers, teachers and safeguarding leads and provides advice about digital terrorist and extremist material.

Government guidance on sharing nudes and semi-nudes (2024) 'This advice is for designated safeguarding leads (DSLs), their deputies, head teachers and senior leadership teams in schools and educational establishments.

A government 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. Sign up to CASPAR at www.nspcc.org.uk/caspar The NSPCC also provide training www.nspcc.org.uk/training