Ark Ayrton Primary Academy

Online Safety Policy

Date of last review:	July 2023	Author:	S Bennett-Acres
Date of next review:	July 2024	Owner:	Head of Safeguarding
Type of policy:	☐ Network-wide ☐ Set for school ☒ Tailored by school	Approval:	K. Oliver Chair of Gov
School:	Ark Ayrton Academy	Key Contact Name:	Mandy Rutledge/ Rachel Down
Key Contact Email:	Info@arkayrtonprimary.org	Key Contact Phone:	02392824828

POSITIONING WITHIN ARK OPERATIONAL MODEL

Component	Element
☐ Strategic Leadership & Planning ☐ Monitoring, Reporting & Data ☐ Governance & Accountabilities ☐ Teaching & Learning ☐ Curriculum & Assessment ☒ Culture, Ethos & Wellbeing ☐ Pathways & Enrichment ☐ Parents & Community ☐ Finance, IT & Estates ☐ Our People	Online Safeguarding

Key Contacts - Ark Ayrton Academy

In the event you need to talk to any of the below named key contacts, please call on the below telephone number and ask to speak to the key person named below:

- School contact number – 02392824828

Ark Ayrton Academy –Safeguarding Key Contacts		
Name	**Role**	**Email**
Sophie Bennett-Acres	Head of School	Info@arkayrtonprimary.org
Sophie Bennett-Acres	**Designated Safeguarding Lead (DSL)**	Info@arkayrtonprimary.org
Kate Magliocco	Regional Director	Kate.magliocco@arkayrtonprimary.org
Joycelyn Thomas	Ark's Head of Safeguarding	Joycelyn.Thompson@arkonline.org
Katie Oliver	Safeguarding Link Governor	Governors can be contacted through the clerk. The current Clerk to Governors is Valerie Oldfield Info@arkayrtonprimary.org
Katie Oliver	Chair of Governors	
Carole Fenton	SENCo	Info@arkayrtonprimary.org
Miranda Tabraham	Senior Mental Health Lead	Info@arkayrtonprimary.org
Rachel Down	Digital Learning Lead (DLL)	Info@arkayrtonprimary.org
Mandy Rutledge	Student Support/Welfare Manager/DDSL	Info@arkayrtonprimary.org
Lauren Boxall	Attendance Officer	Info@arkayrtonprimary.org
Tegan Asiri	Personal Development/PSHE Lead	Info@arkayrtonprimary.org

Contents

1. Introduction

It is recognised by Ark Ayrton Academy that the use of technology presents challenges and risks to children and adults both inside and outside of school. The online world provides everyone with many positive opportunities; however, it can also present risks in respect of harm arising out of conduct, content, contact and commercialisation (see sec. 3 for further details).

An effective approach to online safety empowers schools to protect and educate children, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Ark Ayrton Academy has allocated responsibilities of safeguarding to the role of Designated Safeguarding Lead (DSL), which includes acting as a point of contact for online safety, and for which they undergo specific training.

This Online Safety Policy and procedures is used in conjunction with other school policies including the Safeguarding and Child Protection Policy, Data Protection Policy, Behaviour Policy and Anti-bullying policy.

Although it is impossible to eliminate risks completely, good educational provision will build students' resilience and give them the confidence and skills manage these risks. This policy explains how we provide safeguards to help students manage and reduce those risks and be safe and responsible users of digital technology.

1.1 Policy statement

Ark Ayrton is committed to the effective and purposeful use of technology for teaching, learning and administration and to protecting its students, staff, parents, and visitors, from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.

The school actively promotes the participation of parents to help the school safeguard the welfare of students and promote the safe use of technology.

1.2 Aims and objectives

This policy aims to:

- Set out expectations for all Ark Ayrton students and staff online behaviour and activities using digital technology (including when devices are offline).
- Set the standard of online behaviour that must be upheld both inside and outside school, regardless of the device or platform.
- Facilitate the safe, responsible, and respectful use of technology to support teaching and learning.
- Prepare children for the risks and opportunities present in the digital world to allow them to stay safe and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology, and the online

world, for the protection and benefit of the children and young people in their care.
- Establish clear codes of conduct for online behaviour of staff and students and procedures to follow

This policy applies to staff including the governing body, teachers, support staff, external contractors, visitors, volunteers (and other individuals who work for or provide services on behalf of Ark Ayrton) as well as students and parents/carers.

1.3 Communication of the policy

To ensure the successful implementation of this policy it is essential that its aims and objectives are communicated to staff, students, and the wider community in the following ways:

- Posted on the school website.
- Policy and procedures to be discussed as part of the school induction pack for new staff, including the staff Acceptable Use Agreement.
- Included in relevant safeguarding training

1.4 Policy development, monitoring and review

The policy, procedures and guidance on online safety have been developed by the Safeguarding Team made up of:

- Head of School and SLT
- Online safety lead/DSL
- Staff – including teachers/support staff/technical staff

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

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of:
    - students
    - parents and carers
    - staff

The policy is reviewed annually by the DSL and with final policy sign off made by the Principal.. The policy will be reviewed sooner if deemed necessary due to significant changes in legislation or government guidance on safeguarding, or because of any other significant event or safeguarding incident.

2. Roles and Responsibilities

Safeguarding and child protection includes online safety and is everyone's responsibility. To ensure the online safeguarding of members of Ark Ayrton Academy community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse, as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

2.1 Local Governing Body (LGB)

The role of the Local Governing Body / Safeguarding Link Governor:

- Support the school in encouraging parents and the wider community to become engaged in online safety activities.

2.2 Regional Directors

The role of the Regional Director:

- To receive updates from the Principal and DSL on how students are taught how to keep themselves safe, including online, as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.
- To note the Online Safety Policy and to be kept abreast on the effectiveness of the policy in line with the UKCIS document 'Online Safety in Schools and Colleges: questions from the governing body'.

2.3 Head of School

The Head of School has overall responsibility for online safety provision, and responsibilities include:

- Ensuring the online safety of members of the school community and fostering a culture of safeguarding, with day-to-day responsibility for online safety delegated to the DSL.
- The Principal to have regular reviews with the DSL and incorporate online safety into discussions of safeguarding at Regional Director meetings.
- Oversee the activities of the DSL and ensure that the DSLs responsibilities in relation to online safety, listed below, are followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Ensure that all staff undertake safeguarding and child protection training (including online safety) at induction which is regularly updated.
- Ensure that appropriate filters and monitoring systems are in place, with consideration given to 'over-blocking' which may lead to unreasonable restrictions.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and make all staff aware of procedures to be followed.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.

- Be responsible for ensuring that all staff receive suitable training to carry out their role in safeguarding children online.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of students for online safety issues.
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.

2.4 Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for safeguarding and child protection (including online safety) with day-to-day responsibility for online safety issues.
- Be aware of the potential for serious child protection concerns that can arise through online harms.
- Recognise additional risks that pupils with Special Educational Needs or Disabilities (SEND) face online.
- Ensure an effective approach to online safety is in place that empowers the school to protect and educate the whole school community in their use of technology, and establish mechanisms to identify, intervene, and escalate any incident where appropriate.
- Promote an awareness of online safety to parents throughout the school community, including parents.
- Liaising with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated.
- Keep up to date with the latest trends and issues in online safety and review the online safety policy accordingly.
- Communicate regularly with SLT and the designated safeguarding link Governor to discuss current issues, reviews of incidents and filtering logs.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and that these are logged in the same way as any other child protection incident.
- Oversee and discuss appropriate filtering and monitoring with Governors and ensure staff are aware of its necessity.
- Ensure that appropriate filters and monitoring systems are in place, with consideration given to 'over-blocking' which may lead to unreasonable restrictions.

2.5Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education program. This will be provided through a mapped cross-curricular programme, assemblies, pastoral programmes and relevant national initiatives and opportunities such as, Safer Internet Day, Anti-bullying week, etc.

This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that students face. This includes how to use technology safely, responsibly, respectfully, and

securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

2.6 All staff

All staff responsibilities:

- They have an awareness of current online safety trends and threats.
- Understand that online safety is a core part of safeguarding.
- Read, understand, and have signed the staff acceptable use agreement.
- Immediately report any suspected misuse of technology or online safeguarding concern to the DSL in line with the school safeguarding procedures.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure that students understand and follow the Online Safety Policy and acceptable use agreements.
- Supervise and monitor the use of digital technologies, mobile devices, etc., in lessons and other school activities and follow policies regarding those devices.
- In lessons where internet use is pre-planned, learners should be guided to sites checked as suitable for their use, and processes are followed dealing with any unsuitable material that is found in internet searches.
- Have a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, hatred etc.,
- Model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2.7Students

- Read, understand, sign, and adhere to the student acceptable use policy.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policy cover actions out of school, including on social media.
- Understand the benefits, opportunities, risks, and dangers of the online world and know who to talk to at school or outside school if there are problems.

2.8 Parents and carers

- Read and promote the student acceptable use agreement and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media.
- Responsible behaviour includes not sharing images or personal details without permission and refraining from posting negative, threatening, or violent

comments about others, including the school staff, volunteers, governors, contractors, students or other parents and carers.

3. Online Harms

Online harms are user generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person. Online harms can be illegal, or they can be harmful to a child or vulnerable adult, but still be legal. It is essential that children are safeguarded from potentially harmful and inappropriate online material.

Examples of online harms include:

- Online child sexual exploitation or grooming
- Viewing harmful content
- Sharing nudes
- Online bullying
- Online gambling

The breadth of issues classified within online safety is considerable and ever evolving, 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: peer to peer pressure, commercial advertising and adults posing as children with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: 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.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3.1 Online Child Sexual Abuse

Sexual abuse can happen online as well as offline and includes:

- showing pornography
- exposing a child to sexual acts
- forcing a child to make, view or share child abuse images or videos
- making, viewing, or distributing child abuse images or videos
- forcing a child to take part in sexual activities or conversations online

Online child sexual exploitation occurs when a child is sexually exploited online. They may be persuaded or forced to create sexually explicit photos or videos or have sexual conversations.

The internet has not created child sexual abuse, but it makes it easier for adult offenders to contact and groom children and young people. When contacting a child online, an adult offender's objective might be to meet them fact to face to abuse them. Many offenders, however, abuse children without meeting them by forcing or tricking them into producing and sharing sexual images or videos or engaging in sexual activity on camera or livestream.

Staff should always remain vigilant and observant to this type of abuse. Offenders of child sexual abuse come from all walks of life. Perpetrators although predominantly male, can also be female, young, or old, and from any social or cultural background. They can abuse children of any gender, age and social or cultural background. They can also be people that the child knows.

3.2 Grooming Behaviour

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation, or trafficking. Children and vulnerable adults can be groomed online or face-to-face, by a stranger or by someone they know, for example a family member, friend or professional. Groomers may be male or female of any age.

It can be difficult to tell if a child is being groomed as the signs not always obvious and may be hidden. Older children might behave in a way that seems to be "normal" teenage behaviour, masking underlying problems. A child is unlikely to know they have been groomed. They might be worried or confused and less likely to speak to an adult they trust.

Some of the signs you might see include:

- being very secretive about how they are spending their time, including when online
- having an older boyfriend or girlfriend
- having money or new things like clothes and mobile phones that they cannot or won't explain
- underage drinking or drug taking
- spending more or less time online or on their devices
- being upset, withdrawn, or distressed
- sexualised behaviour, language, or an understanding of sex that is not appropriate for their age
- spending more time away from home or going missing for periods of time.

Grooming is a criminal offence and occurs where an adult engages in sexual communications that relates to sexual activity and communications for the purpose of obtaining sexual gratification (Serious Crime Act 2015, part 67).

3.3Child Sexual Abuse Material (CSAM)

Child sexual abuse material is a result of children being groomed, coerced, and exploited by their abusers, and is a form of child sexual abuse. It is important to use the correct term ‘child sexual abuse material’ (CSAM) and not ‘child pornography’ which implies it is a sub-category of legally acceptable pornography, rather than a form of child abuse and a crime.

It is a serious criminal offence against children to take, make, distribute, or possess an indecent photograph or pseudo-photograph of a child under the age of 18.

Child sexual abuse material can remain online indefinitely, therefore children continue to be re-victimised each time it is viewed, shared, or downloaded.

Children who have been abused in this way may grow up with feelings of shame, guilt, humiliation, and fear that abuse materials may resurface in future, giving them no sense of closure for the crimes committed against them.

3.4 Sharing Nudes

Sharing nudes or semi-nudes is a term used to describe when persons under 18 send or post nude or semi-nude images, videos, or livestreams online.

Professionals might use:

- Sexting
- Youth-produced sexual imagery
- Self-generated indecent imagery

Young people might use:

- Nudes
- Pics
- Dick pics

3.4.1 Child protection referral:

Some young people might share nude imagery consensually as a way of exploring their sexuality. This can form part of a healthy relationship if it is consensual and appropriate for their age and stage of development.

However, it is important that any incident involving children and nudes is considered a potential safeguarding concern.

An incident should always result in a child protection referral if:

- The incident involves an adult.
- There is reason to believe that a child or young person has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent (e.g., learning disability).
- The image depicts sexual acts not appropriate for the young person's development stage or are violent.
- The images depict sexual acts with any child under 13.
- Reason to believe that the child is in immediate risk of harm due to the sharing of the image, e.g., presenting as suicidal or self-harming.

3.4.2 Report Remove

Report Remove is a tool that allows young people to report an image or video shared online, to see if it's possible to get it taken down. Provided by Childline and IWF, it keeps the young person informed at each stage of their report and provides further support where necessary. Report Remove can be accessed by visiting https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/

3.5 Harmful Content

As children start to explore the internet, they may come across content that is not suitable for their age, or that may upset or worry them

Harmful content can include:

- Sexual content, including pornography
- Violent content
- Fake news
- Hate speech

Content may be legal but could be harmful to a child. Harmful content can depend on a child's age, development, maturity, and support.

3.5.1 Pornography

Legal adult pornography is readily available online. It can be found via search engines, but often it appears in pop ups. Having, sharing, or selling adult pornography is, as a general rule, not illegal. However, some extreme pornography is illegal and possessing, making, or distributing it are serious offences.

A note that it is not illegal for someone under the age of 18 to watch pornography, it is illegal for someone to show, or give access to pornography to anyone under 16.

3.5.2 Extreme pornography

It is illegal to possess 'extreme pornographic images'. This is material that's 'grossly offensive, disgusting or otherwise obscene', and that 'explicitly and realistically' shows:

- life threatening injury,
- serious injury to a person's anus, breasts, or genitals,
- bestiality (a sexual act with an animal),
- necrophilia (a sexual act with a human corpse),
- rape or assault by penetration.

3.5.3 Effects on children:

- Normalisation of extreme or risky sexual acts
- More likely to engage in harmful sexual activity
- Developing discriminatory attitudes
- Inability to engage in real-life relationships
- An unhealthy preoccupation with pornography which can interfere with other aspects of life

Some young people speak of being "obsessed" or "addicted" to certain online material, most notably pornography. For some, visiting adult sites had become part of their daily routine.

Ark Ayrton Academy staff should be aware of children's use of the internet and interacting online, and any concerns should be forwarded to the DSL.

3.6 Self-harm and suicide

Many online forums, social media, messaging apps and websites can glorify, reinforce, or encourage self-harming or suicidal behaviour. Content includes information, pictures, or videos on how to self-harm and describe ways in which children and young people can take their own lives.

The reasons children and teenagers can self-harm are often complicated and will be different for every child or young person. Sometimes a child or teenager may not know the reasons they self-harm. For many young people, self-harm can feel like a way to cope with difficult feelings or to release tension. The physical pain of hurting themselves can feel like a distraction from the emotional pain they are struggling with.

Some difficult experiences or emotions can make self-harm more likely in children:

- experiencing depression, anxiety or eating problems
- having low self-esteem or feeling like they are not good enough
- being bullied or feeling alone
- experiencing emotional, physical, or sexual abuse, or neglect
- grieving or having problems with family relationships
- feeling angry, numb or like they do not have control over their lives.

Any concerns about a child or vulnerable adult should be communicated to the DSL.

3.7Online Bullying

Bullying is behaviour that hurts someone else and includes name calling, hitting, pushing, spreading rumours, threatening, or undermining someone. Online bullying, often referred to as cyberbullying, can occur on any type of device connected to the internet, including social networks, gaming, and websites.

Some examples:

- Abusive or threatening messages or emails
- Abusive comments on social media
- Sharing humiliating videos or pictures of someone
- Spreading rumors online
- Trolling – the sending of menacing or upsetting messages on social networks, chat rooms or online games
- Excluding children from online games, activities, or friendship groups

3.7.1 Signs of bullying

No single sign will indicate for certain that a child is being bullied, but watch out for:

- belongings getting 'lost' or damaged,
- physical injuries, such as unexplained bruises,
- being afraid to go to school, being mysteriously 'ill' each morning, or skipping school
- not doing as well at school,
- asking for, or stealing, money (to give to whoever is bullying them),
- being nervous, losing confidence, or becoming distressed and withdrawn,
- problems with eating or sleeping,
- bullying others.

3.7.2 Vulnerability factors

Disabled children can experience bullying because they can be seen an easy target and less able to defend themselves.

This might be because of their:

- physical appearance
- race
- faith or culture
- gender identity
- sexuality
- disability or additional needs

3.7.3 How to help a child experiencing online bullying

- Reassure them you are there to help
- Help them to block and report
- Show them how to save evidence by taking screenshots
- Remind them never to retaliate
- Let them know they can always talk to you or Childline

3.7.4 Responding to incidents

- Listen to all the children involved to establish what has happened.
- Record details of the incident and any actions you have taken.
- Inform the DSL.
- Inform parents and carers (unless doing so would put a child at further risk of harm)
- Provide support to the child/children being bullied, children who witnessed the bullying and the child/children who has been accused of bullying.
- Ask the child/children who have been bullied what they would like to happen next.
- Consider appropriate sanctions for children that have carried out bullying.
- Continue to monitor the situation even if the situation has been resolved.

3.7.5 Preventing bullying

Ark XX Academy build in contextual safeguarding considerations into their operating systems and risk assessment, including:

- Consider whether there are any areas where bullying may be more likely to happen, e.g., toilets or unsupervised areas.
- Staff awareness of dynamics of children's relationships.
- Talking to children and young people where suspected issues arise.

At Ark XX Academy within our learning, we create an inclusive and supportive environment where children, young people and adults treat each other with respect. As part of this, staff and volunteers should challenge inappropriate behaviour or language and not dismiss it as 'banter'.

3.8 Online Gaming

Online games can be a great way for children and young people to keep busy and stay in touch with friends and family, but it is important that they play safely.

Gaming can be a positive thing providing a way for children to, relax, socialise, learn new skills, be part of a team. However, it also carries risks.

- Grooming by online predators.
- Online bullying.
- Violent content extreme violence, warfare, and criminal activity.
- Show explicit sexual acts, which may glamourise rape and sexual assault.
- Use racist, homophobic, or sexist language, or swearing.
- Depict certain groups such as women in a derogatory way.
- Online Gambling.

More information on the risks of online gaming and a short video can be found on the NSPCC website.

3.9 Online Radicalisation and Extremism

Children can be exposed to different views and receive information from various sources. Some of these views may be considered radical or extreme. Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is in itself a form of harm.

Ark Ayrton Academy recognise its responsibility to challenge and report radical or extreme content as part of a shared effort to challenge and tackle extremism.

What to do if you think a child is being radicalised:

If you think a child or the people around them are involved in radicalisation and there is an immediate risk of harm, call 999 straight away.

If not an emergency:

- contacting the DSL
- calling the police anti-terrorism hotline on 0800 789 321
- calling the radicalisation helpline
- reporting suspicious activity online at https://act.campaign.gov.uk/

Further information on radicalisation and extremism can be found on the NSPCC website.

4. Safe use of technology

Ark Ayrton Academy is committed to the safe and purposeful use of technology for teaching, learning and administration.

Use of technology should be safe, responsible, respectful to others and legal. Staff, students, parents, and visitors are responsible for their actions, conduct and behaviour when using technology at all times.

The school will support the use of technology and make internet access as unrestricted as necessary whilst balancing the educational needs of our students, the safety and welfare of staff, students, parents and visitors, and the security and integrity of our systems.

Monitoring, logging, and alerting tools are in place to maintain technology safety, safeguarding and security for the protection of staff, students, parents and visitors.

Technology has become a fundamental part of education, not only as the vehicle to deliver great teaching and learning, but as a platform for collaboration and productivity. We want students to enjoy using technology and to become skilled users.

Students will be educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

The school actively encourages the participation of parents to help promote the safe use of technology with their children.

Any concern regarding unsafe or inappropriate use of technology should be reported to a teacher, or DSL as soon as possible.

5. Handling online safety concerns and incidents

The school procedures for dealing with safeguarding concerns, which includes those arising from online safety, are detailed in the Safeguarding and Child Protection Policy.

This school commits to take all reasonable precautions to ensure that students are safe online but recognises that incidents will occur both inside school and outside school. Incidents that occur outside school will continue to impact on students when they come into school. All members of the school are encouraged to report issues swiftly to allow for a quick and sensitive escalation processes.

Any suspected online risk or safeguarding concern should be reported to the DSL. Any concern or allegation about staff misuse should be referred directly to the Head of School, unless the concern is about the Head of School or Executive Head, in which case the complaint is referred to the Regional Director.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

The school will actively seek support from other agencies as needed, e.g., the local authority, NSPCC, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Police or IWF).

6. Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Principal, and staff authorised by them, have a statutory power to search students and possessions on school premises. This includes the content of mobile phones and other devices, where there is a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

7. Filtering and Monitoring

At Ark Ayrton Academy we manage this risk by:

When students use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems, SENSO. This is a cloud-based

solution that allows us to monitor, regularly review and manage all computers and pupils throughout the network from a centralised web portal in real time for their effectiveness.

However, many pupils are able to access the internet using their own data plan as many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G). This access means some children, whilst at school could sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.

To minimise inappropriate use, at Ark Ayrton Academy pupils sign an acceptable use agreement.

As we recognise that personal mobile phones and smart technology have the potential to be used inappropriately Ark Ayrton Academy has developed guidance to outline the required protocol for all employees, pupils, supply, volunteers, governors, and parents/carers. Staff, volunteers, parents, or pupils must not use personal phones or devices to take pictures of pupils while in the school environment or on educational visits.

For further information on the use of mobile phones, smart technology, cameras and sharing of images please see Ark IT Acceptable Use Agreement.

Ark Ayrton Academy will also:

Ensure appropriate filters and monitoring of devices. Whilst it is essential to ensure that appropriate filters and monitoring systems are in place, Ark Ayrton Academy will be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught (*DFE Guidance).

Ensure robust safeguarding support and follow up is in place to act on any issues raised from the filtering and monitoring process

8. Network security

Technical security features, such as anti-virus software, are kept up-to- date and managed by the Central IT Team.

- Firewalls are switched on at all times.
- The Central IT Team review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.
- Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- Staff members and pupils report all malware and virus attacks to the ICT Lead and if appropriate, the Principal.
- All members of staff have their own unique usernames and private passwords to access the school's systems.
- All pupils are provided with their own unique username and private passwords.
- Staff members and pupils are responsible for keeping their passwords private.
- Passwords have a minimum and maximum length and require a mixture of characters to ensure they are as secure as possible.
- Passwords resets will be encouraged at least termly.
- Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.
- Users are required to log out of devices when they are not in use.

- Users inform the appropriate staff if they forget their login details, who will arrange for the user to access the systems under different login details.
- If a user is found to be sharing their login details or otherwise mistreating the password system, the procedures in the Acceptable Use Agreement will be followed.
- Chain letters, spam and all other emails from unknown sources are deleted without being opened.
- Online safety training will explain what a phishing email and other malicious emails might look like.
- Any cyberattacks initiated through emails are managed by Central IT Team.
- Full details of the school's network security measures can be requested from the Central IT Team.

9. Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated annually along with regular online safety updates as required.

In addition to this training, the DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years as well as regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

• Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.

• Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

10. Related policies

Safeguarding and promoting the welfare of children and vulnerable adults is a broad concept. Other Ark Ayrton Academy policies and procedures that contribute to safeguarding children and vulnerable adults should be read in conjunction with this policy.

Safeguarding and Child Protection Policy
Behaviour Policy
Anti-Bullying Policy
Mental Health and Wellbeing Policy
Managing Allegations against Staff
Disciplinary Policy
Attendance Policy
Data Protection Policy

11. Legal Framework

This policy has been drawn up based on UK/English law, policy, and guidance.

United Nations Convention on the Rights of the Child 1991
Protection of Children Act 1978
Children Act 1989 and 2004
Sexual Offences Act 2003
Female Genital Mutilation Act 2003
Safeguarding Vulnerable Groups Act 2006
Protection of Freedoms Act 2012
Communications Act 2003
Malicious Communications Act 1988
Counter Terrorism and Security Act 2015
Serious Crime Act 2015
Modern Slavery Act 2015
Defamation Act 2013
Digital Economy Act 2017
Data Protection Act 2018, GDPR 2018
Privacy and Electronic Communications Regulations (PECR)
HM Government (2018) Working Together to Safeguard Children
Voyeurism Act 2019
Communications Act 2003
Malicious Communications Act 1988