

Orchard Head Primary School Online Safety Policy 2026-2027

Date of last review:	August 2026	Author:	Jane Baldwin
Date of next review:	August 2027	Owner:	Head of Safeguarding
Type of policy:	☐ Network-wide ☐ Set for school ☒ Tailored by school	Approval:	Management Team
School:	Orchard Head Primary School	Key Contact Name:	Claire Hughes
Key Contact Email:	OHS.Admin@arkorchardhead.org.uk	Key Contact Email:	Claire.Hughes@arkonline.org

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 – Orchard Head Primary School

In the event you need to contact any of the below named key staff, please use the appropriate email address:

School contact number – 01977 723495

Orchard Head Primary School – Safeguarding Key Contacts		
Name	Role	Email
Kara Adams	Principal	KAdams@arkorchardhead.org.uk
Maria Stubbs	Designated Safeguarding Lead (DSL)	MStubbs@arkorchardhead.org.uk
Julian Appleyard	Regional Director	Julian.Appleyard@arkonline.org
Ian Shuttleworth	Executive Principal	IShuttleworth@arkhalfpennylane.org.uk
Jane Baldwin	Ark Head of Safeguarding	Jane.Baldwin@arkonline.org
Caz Brasenell	Regional Director (Birmingham)	Caz.Brasenell@arkonline.org
Maria Stubbs	Inclusion Leader	MStubbs@arkorchardhead.org.uk
Kara Adams	Principal	KAdams@arkorchardhead.org.uk

Contents

1. Introduction	4
1.1. Policy statement	4
1.2. Aims and objectives.....	4
1.3. Communication of the policy	5
1.4. Policy development, monitoring and review.....	5
2. Roles and Responsibilities.....	6
2.1. Principal.....	6
2.2. Designated Safeguarding Lead (DSL)	6
2.3. Curriculum Leads.....	7
2.4. All staff.....	8
2.5. Pupil's	8
2.6. Parents and carers.....	9
2.7. Regional Director.....	9
2.8. School Performance Review Board (SPRB)	9
3. Online Harms	9
3.1. Online Child Sexual Abuse	10
3.2. Grooming Behaviour	11
3.3. Child sexual abuse material (CSAM)	11
3.4. Self-generated intimate images (including AI-generated 'deepfakes')	11
3.4.1. Child protection referral:.....	12
3.4.2. Report Remove	12
3.5. Harmful Content.....	12
3.5.1. Sexual content, including pornographic, simulated or AI-generated imagery	12
3.5.2. Extreme content including pornography, simulated or AI-generated imagery.....	13
3.5.3. Effects on children:.....	13
3.6. Self-harm and suicide	13
3.7. Online Bullying, harassment and coercive behaviour	13
3.7.1. Signs of bullying, harassment and coercion	14
3.7.2. Vulnerability factors	14
3.7.3. How to help a child experiencing online bullying, harassment or coercion.....	14
3.7.4. Responding to incidents.....	15
3.7.5. Preventing bullying	15
3.8. Online Gaming.....	15
3.9. Online Radicalisation and Extremism	15
3.10. AI-Generated Content and Deepfakes.....	16
4. Safe use of technology	16
5. Handling online safety concerns and incidents	17
6. Searching and confiscation	17
7. Filtering and Monitoring.....	17
8. Network security.....	18
9. Staff training	19
Related policies.....	19
10. Legal Framework.....	20

1. Introduction

It is recognised by Orchard Head Primary School 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.

Orchard Head Primary School Designated Safeguarding Lead (DSL) acts as the school's lead for online safety, maintaining a working understanding of Ark's filtering and monitoring systems and contributing to the annual review of their effectiveness, including for vulnerable pupil's. The DSL ensures that responsibilities across governors, senior leaders, staff and IT support are clearly defined to meet Department of Education (DfE) Filtering and Monitoring Standards, and that illegal content is always blocked with updated controls in place through South West Grid for London (SWGfL) and SENSO. The DSL also ensures timely monitoring alerts via SENSO are reviewed in line with safeguarding procedures and works with IT and data protection leads to maintain robust information security and access controls.

This Online Safety Policy and procedures is used in conjunction with other school policies including the Safeguarding and Child Protection Policy, Ark's IT and AI Acceptable Use Policy, Data Protection Policy, Behaviour Policy, Anti-bullying Policy and staff Code of Conduct.

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

1.1. Policy statement

Orchard Head Primary School is committed to the effective and purposeful use of technology for teaching, learning and administration, and to protecting its pupil's, 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/carers to help the school safeguard the welfare of pupil's and promote the safe use of technology.

1.2. Aims and objectives

This policy aims to:

- Set out expectations for all Orchard Head Primary School pupil's 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.

- Enable parents/carers to have a greater understanding of online risks and how to facilitate safe access to the online world.
- Establish clear codes of conduct for online behaviour of staff, pupil's, and procedures to follow the school Behaviour and Relationships policy, Anti-Bullying Policy, Staff Code of Conduct, Acceptable Use Agreement and Home School Agreement as found on our school website.

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 Orchard Head Primary School as well as pupil's 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, pupil's, 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.
- The school communicates the acceptable usage agreement through curriculum input, assemblies, drop down events and safer internet curriculum.
- Included in relevant safeguarding training.
- The school raises awareness with parents as part of induction, through newsletters and regular communication.

1.4. Policy development, monitoring and review

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

- Principal and Senior Leadership Team (SLT/DSL)
- Head of Safeguarding
- Director of Technology
- Digital Innovation Lead
- Digital Strategy Lead

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

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:
 - pupil's
 - parents and carers
 - staff

The policy is reviewed annually but may take place 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 where lessons are learnt.

2. Roles and Responsibilities

Safeguarding and child protection includes online safety and is everyone's responsibility. To ensure the online safeguarding of members of Orchard Head Primary School 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. Principal

The Principal 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.
- Consult regularly with the DSL on online safety matters, ensuring issues, updates and best practice are discussed and incorporated into safeguarding and teaching reviews at Regional Director meetings.
- Oversee the activities of the DSL and ensure that the DSL's responsibilities in relation to online safety (listed below), are followed and fully supported.
- Ensure that all staff follow policies and procedures.
- Ensure that all staff undertake safeguarding and child protection training (including Ark online safety and cybercrime module) 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.
- 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 pupil's for online safety issues.
- Supporting staff to ensure online safety is embedded throughout the curriculum.
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.

2.2. 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 as outline in the Safeguarding and Child Protection Policy 2026.
- Undertake appropriate online safety training.

- Be aware of the potential for serious child protection concerns that can arise through online harms including:
 - Online misogyny and content that normalises harmful sexual behaviour
 - Financial exploitation and online scams, including financially motivated sextortion
 - AI-generated intimate imagery (deepfakes) and synthetic media used to harass, coerce or defraud
- Recognise additional risks that pupil's with Special Educational Needs or Disabilities (SEND) face online, including those who may complete remote learning.
- Ensure an effective and responsive 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.
- Have oversight of online safety training arrangements to ensure all staff are appropriately trained and that learning from emerging themes and risks is reflected in practice.
- Communicate regularly with SLT and the designated safeguarding link Governor to discuss current issues, reviews of incidents and filtering logs.
- Ensure that all staff and pupils 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 filtering and monitoring arrangements to ensure appropriate systems are in place, staff understand their importance and consideration is given to avoiding unreasonable restrictions through over-blocking.
- Stay informed about the use of AI technologies in the school environment, including generative AI tools.
- Work collaboratively with external agencies in response to online safety concerns when required.

2.3. Curriculum Leads

Appropriate 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. and has the capability to adapt in response to emerging themes.

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 pupil's 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.

Curriculum Leads will ensure that AI literacy is embedded in the Online Safety curriculum, including understanding how AI systems work, their limitations, and how to critically evaluate AI-generated content.

2.4. All staff

All staff should :

- Have an awareness of current online safety trends and threats.
- Understand that online safety is a core part of safeguarding.
- Complete the Ark Online Safety & Cybercrime Module.
- Read, understand, and have signed the staff Acceptable Use Agreement.
- Never use own devices to communicate with pupil's without authorisation from the Principal in exceptional circumstances.
- Model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- Report any websites or online safety concerns immediately through the Halo Service Desk by raising a "Report a Website or Online Safety Issue" ticket,

- Go to <https://servicedesk.arkonline.org/portal/home>

They must also:

- Inform the Designated Safeguarding Lead (DSL).
- Log on CPOMS
- Immediately report any suspected misuse of technology or online safeguarding concern to the DSL in line with the school safeguarding procedures.
- Ensure online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure that pupil's understand and follow the Ark Online Safety Policy and Acceptable Use Agreements.
- Supervise and monitor the use of digital technologies and permitted devices e.g., in lessons and other school activities including school trips/residentials 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.,
- Be aware of the risks and benefits of AI tools used in teaching and learning, and ensure pupils are guided in their safe and responsible use, where appropriate.

2.5. Pupil's

All pupils should:

- Read, understand, sign, and adhere to the pupil Acceptable Use Agreement.
- 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 benefits and risk of the online world, use digital technologies safely and responsibly in and outside school, recognising that the Acceptable Use Agreement applies to online behaviour, including social media, and know where seek support if concerns arise.

- Understand that any inappropriate use of online platforms, including AI tools, which causes harm or distress to adults or children will be addressed in line with the Ark Schools (Pontefract Region) Behaviour Policy and any associated policies and procedures.

2.6. Parents and carers

Parents and carers are expected to:

- Read and promote the pupil Acceptable Use Agreement and encourage their children to follow it.
- Support Orchard Head Primary School's smartphone free approach.
- Adhere to school's expectations regarding wearable devices when on site.
- Consult with the school if they have any concerns about their children's and others' use of technology.
- Refraining from posting unauthorised images or negative, threatening, or violent comments about Orchard Head Primary School staff and other members of the school community.

2.7. Regional Director

The role of the Regional Director:

- To receive updates from the Principal and DSL on how pupils are taught 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 UK Council for Child Internet Safety (UKCIS) document [‘Online Safety in Schools and Colleges: questions from the governing body’](#).

2.8. School Performance Review Board (SPRB)

The role of the SPRB / Safeguarding Link Governor:

- To review effectiveness of filtering and monitoring arrangements at least annually. As part of standardised visit, governors will provide oversight, review and challenge. [Cyber security standards for school and colleges 2026](#)
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.

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 and therefore considered a potential safeguarding concern. 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, violent, extremist or adult content including sexual imagery
- Fake news and mis/disinformation
- Self-harm and suicide content
- Self-generated intimate images including AI generated ‘deepfakes’ (language such as ‘youth produced sexual imagery’ or ‘sexting’ may still be heard but not referenced in this policy)
- Extremist content

- Misogyny and misandry
- Online bullying, threats, coercion or harassment
- Online gambling
- Hacked accounts
- Privacy violations
- Impersonation

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, disinformation, racism, misogyny/misandry, extreme sexual or physical violence, self-harm, suicide, anti-Semitism, radicalisation, and extremism. This policy recognises the link between online misogyny and harmful sexual behaviour. Staff must challenge and report misogynistic content or language and act early to prevent escalation.
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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 (including AI generated images), 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 (including AI generated)
- 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 face 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 are 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).

3.3. Child sexual abuse material (CSAM)

Child sexual abuse material (CSAM) 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.

CSAM 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. Self-generated intimate images (including AI-generated 'deepfakes')

Self-generated intimate images (including AI generated 'deepfakes') is a term used to describe when a person under 18 sends or posts nude or semi-nude images, videos or livestreams online.

Professionals might use:

- Self-generated intimate images

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, including where images appear to have been created or altered using AI (deepfakes).
- There is reason to believe that a child or young person has been coerced, blackmailed, financially sextorted 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, including where images appear to have been created or altered using AI (deepfakes).
- The images depict sexual acts with any child under 13, including where images appear to have been created or altered using AI (deepfakes).
- Reason to believe that the child is at 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 (Childline and Internet Watch Federation – IWF) 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. The outcome depends on the platform removal policies and IWF assessment. It will keep 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 (including extreme sexual content) and AI-generated imagery
- Violent and weapon related content (including extreme violence)
- Misogyny and gender-based hostility
- Mis- and disinformation, including fake news, conspiracy narratives and AI-generated content
- Hateful (hate speech) and discriminatory

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. Sexual content, including pornographic, simulated or AI-generated imagery

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 content including pornography, simulated or AI-generated imagery

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.

Orchard Head Primary School staff should be aware of children's use of the internet and interacting online, and any concerns should be forwarded to the DSL and recorded on CPOMS.

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 and recorded on CPOMS.

3.7. Online Bullying, harassment and coercive behaviour

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 can include:

- Repeated or targeted use of messages, comments, images or posts to humiliate, exclude or upset a child online.
- Encouraging or involving others to take part in mocking, ridiculing or isolating a child through digital platforms.
- Sending abusive, threatening or unwanted messages (includes use of a pseudonym or a number belonging to someone else), or content that causes distress or fear, even if the behaviour is not repeated.
- Silent phone calls.
- Using online platforms or anonymity to intimidate, degrade or target a child based on personal characteristics or vulnerabilities.
- Pressuring a child to do something online, such as sharing images, information or money, by using threats, guilt or manipulation.
- Controlling a child's online activity through monitoring, impersonation or threats to share private content if demands are not met.

3.7.1. Signs of bullying, harassment and coercion

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 as 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, harassment or coercion

- Reassure them you are there to help
- Record and share concerns with the DSL
- 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, a trusted adult 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 and record on CPOMS
- 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 (if appropriate and in the interest of the child to do so)
- Consider age-appropriate sanctions for children that have carried out bullying in line with the school's Behaviour Policy.
- Consider undertaking appropriate external referrals to prevent repetition and escalation for all parties. This includes notify police where an alleged crime has been committed.
- Continue to monitor the situation even if the situation has been resolved.

3.7.5. Preventing bullying

Orchard Head Primary School builds 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 – 'hotspots', e.g., toilets, stairwells or unsupervised areas.
- Staff awareness of dynamics of children's relationships.
- Talking to children and young people where suspected issues arise.
- Delivery of an effective and responsive curriculum to promote online safety
- Providing opportunities for parents to build their confidence in managing the online world of children safely including knowledge of age-appropriate platforms.

At Orchard Head Primary School, 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

Gaming can be a positive thing, providing a way for children to relax, socialise, learn new skills and 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 can be found on the [NSPCC - Online Games](#)

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.

Orchard Head Primary School recognises 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 or they have been harmed, immediately verbally inform the DSL and log on CPOMS. The DSL is to call 999 if a child is at immediate risk of harm and make subsequent appropriate referrals, including to those listed below.

If not an emergency:

- share with the DSL
- record on CPOMS
- consult with the police anti-terrorism hotline on 0800 789 321
- consult with the 0800 011 3764 Action Counter Terrorism (ACT) - Early Support Line
- report suspicious activity online at <https://act.campaign.gov.uk/>

Further information on radicalisation and extremism can be found on the [NSPCC website](#).

3.10. AI-Generated Content and Deepfakes

AI-generated content, including deepfakes and synthetic media, can be used to deceive, harass, or manipulate. Staff and pupil's should be aware of the potential for AI to create realistic but false images, videos or text, and report any suspicious or harmful content to the DSL immediately.

4. Safe use of technology

Orchard Head Primary School 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, pupil's, 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 pupil's, the safety and welfare of staff, pupil's, 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, pupil's, 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 pupil's to enjoy using technology and to become skilled users.

Pupil's 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.

All AI tools used in schools must be thoroughly vetted for safety, transparency, and data privacy in accordance with Ark's IT and AI Acceptable Use Policy & Agreements 2026/2027 and related DfE guidance including Keeping Children Safe in Education 2026 and Generative AI: product safety standards 2026.

Children should only access Ark authorised AI platforms and any requests for new tools must be submitted via Halo.

Staff must not use AI systems that process pupil data without appropriate consent and a Data Protection Impact Assessment.

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

Further support for professionals working with children and young people, with any online issue can contact the UK Safer Internet Centre Professionals Online Safety Helpline via email 24 hrs a day: helpline@saferinternet.org.uk

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 pupils 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 pupil's when they come into school. All members of the school are encouraged to report issues swiftly to allow for a quick and sensitive escalation process.

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 Principal unless the concern is about the Principal 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.

Online safety concerns and incidents involving an adult, will be responded to in accordance with Ark Allegation Against Staff procedures.

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 pupil's and possessions on school premises, where they have reasonable grounds to suspect that the pupil may have a prohibited item. 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. Instances where it is reasonably believed a criminal offence has taken place; the school will hand an individual's device to the police.

To support the management of Allegations Against Staff procedure, Orchard Head Primary School may access and review school devices, emails, MS Teams communications, files or school managed mobile devices without consent where this is necessary and proportionate. This is carried out solely for the purpose of establishing facts swiftly and fairly, in the best interests of both the child and the staff member involved.

7. Filtering and Monitoring

At Orchard Head Primary School we manage this risk by:

When pupil's use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems – SENSO and South West Grid for London (SWGfL). This is a cloud-based solution that allows us to monitor, regularly review and manage all computers and pupil's throughout the network from a centralised web portal in real time for their effectiveness.

As we recognise that personal mobile phones and smart technology have the potential to be used inappropriately. Ark schools are phone free, which prevents access to mobile and smart technology whilst in school.

To minimise inappropriate use, at Orchard Head Primary School staff and pupil's sign an acceptable use agreement.

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

Orchard Head Primary School will also:

Whilst it is essential to ensure that appropriate filters and monitoring systems are in place, Orchard Head Primary School will be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught ([DfE Guidance: Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard](#)).

Continually review and respond to new and emerging platforms to ensure our filtering process remains robust e.g. AI platforms.

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

Ark Schools:

Ensures appropriate filtering and monitoring systems are in place across all school devices and networks. Filtering and monitoring arrangements are reviewed on an ongoing basis, with a formal review undertaken at least annually to ensure systems remain effective, proportionate and responsive to emerging safeguarding risks, including those arising from new and evolving technologies. Reviews consider the age, needs and vulnerabilities of children, contextual concerns and the working practices of staff. The annual review is a collaborative process involving school Designated Safeguarding Leads, central safeguarding and IT teams, with formal sign off by the Ark Schools Management Team and assurance provided to the Board of Trustees.

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.
- Filtering and monitoring systems are facilitated by SENSO and SWgFL.
- Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- Staff members and pupil's report all malware and virus attacks to the ICT Lead and if appropriate, the Principal.
- All members of staff and pupils have their own unique usernames and private passwords to access the school's systems. These must be kept private.
- Passwords have a minimum and maximum length and require a mixture of characters to ensure they are as secure as possible.
- Password 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 and as part of annual inset. All staff receive and read Part One of Keeping Children Safe in Education 2026.

Online safety training for staff is updated annually along with regular online safety updates as required and in line with emerging risks. Staff annually complete the Ark Online Safety and Cybercrime module which allows staff to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupil's safe while they are online at school. Recognise the additional risks that pupil's with SEND face online and offer them support to stay safe online.
- Understanding of AI technologies, their educational applications, and the safeguarding considerations associated with their use.

Related policies

Safeguarding and promoting the welfare of children and vulnerable adults is a broad concept. Other Orchard Head Primary School 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
Ark Complaints Policy
Anti-Bullying Policy
Mental Health and Wellbeing Policy
Managing Allegations against Staff
Code of Conduct
Ark Disciplinary Policy
Attendance Policy
Ark Data Protection Policy

10. Legal Framework

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

- DfE Keeping Children Safe in Education 2026
- HM Government Working Together to Safeguard Children (2026)
- DfE Generative artificial intelligence (AI) in education (Policy paper 2025)
- DfE Meeting digital and technology standards in schools and colleges (March 2022, update April 2026)
- United Nations Convention on the Rights of the Child 1991
- Online Safety Act 2023
- 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 (DPA) 2018, UK General Data Protection Regulation (UK GDPR)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR)
- Voyeurism Act 2019
- DfE Searching, Screening and Confiscation advice for school 2022
- DfE Teaching online safety in schools guidance (updated 2023)