Online Safety Policy

Policy Lead:	**Assistant Headteacher**
Last Review Date:	September 2024
Next Review Date:	September 2026
Approval needed by:	**Headteacher**

THE **LEARNING** PARTNERSHIP

Monitoring and Revision due:

The online safety policy will be reviewed annually. It will also be reviewed to align with national, regional and local legislative or statutory changes.

This policy links with other policies including;

- Whistleblowing
- Bullying Prevention
- Acceptable Use
- Behaviour and Rewards
- Safeguarding Policy
- Code of conduct
- Complaints
- Data Protection

Disclaimer

Every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance. If errors are brought to our attention, we will correct them as soon as is practicable.

CONTENTS

1. Introduction

Online safety in schools is of paramount importance. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

School staff and trustees play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can.

This policy is applicable to all members of The Oaks Academy. This includes, staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of the school's digital technology systems, both internally and externally within the home and community setting.

2. Online Safety School Statement

The Oaks Academy asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

The Oaks Academy believes that the internet and associated devices are an integral part of everyday life.

The Oaks Academy affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

3. Policy Scope

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports schools in meeting statutory requirements as per the DfE guidance in Keeping Children Safe in Education (KCSiE) (September 2024) and Working together to safeguard children (July 2018) along with non-statutory guidance; Meeting Digital and Technology standards in schools (March 2023), Teaching Online Safety in schools (January 2023) and Safer Recruitment
Consortium; Guidance for safer working practice for those working with children and young people in education settings (February 2022).

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.
Defining online abuse: "*Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones"* (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- cyberbullying
- emotional abuse
- grooming
- sexting
- sexual abuse
- sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- neglect
- sexual
- physical
- emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child

- causing a child to view images or watch videos of a sexual act.

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance as stipulated on page 1-2 of this policy.

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within The Oaks Academy.

4.1 Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; headteacher, teachers, substitute teachers, work-experience staff, office staff, nurses, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.

4.2 Governors and Senior Leadership Team

This should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

4.3 Designated Safeguarding Lead (DSL), Digital Safeguarding Lead and the Deputy Designated Safeguarding Lead (Deputy DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.

- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the senior leadership team.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.

- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

4.4 Children and Young People

With respect to online safety in your school, children need to:

- Know who the DSL is.
- Engage in age appropriate online safety education opportunities.
- Contribute to policy development and review.
- Read and adhere to online safety policies.
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Where and how to find help with any online incidents or concerns.
- How, when and where to report concerns and when to seek help from a trusted adult.

4.5 Parents and Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse.

5. Education and Training

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of children and young people relies upon constructive relationships that are conducive to robust multi- agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of four categories:

Contact: Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Commerce: Risks such as online gambling, inappropriate advertising, phishing or financial scams.

5.1 Learners

The Oaks Academy will promote safe and responsible internet use:

- Education regarding safe and responsible use and access of the internet.
- Include online safety in Personal, Social, Health and Economic (PSHE) education, Relationships and Sex Education (RSE) and Information Computer Technology studies.
- Reinforce online safety messages as a continuum.

The Oaks Academy will support learners understanding based on age and ability:

- Informing all learners of monitoring and filtering in place.
- Implement peer education strategies.
- Provide continuous training and education as part of their transition across key stages.
- Use alternative, complementary support where needed.
- Seeking learner voice.

5.2 Vulnerable Learners

Vulnerable children who need our help the most are not only missing out on opportunities to flourish online but are often experiencing the very worst that the online world can be. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

The Oaks Academy recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

The Oaks Academy will ensure the effective and safe provision of tailored online safety education.

The Oaks Academy will obtain input and advice from specialist staff as deemed necessary.

5.3 Staff

The Oaks Academy will:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Complete up to date online safety training in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure training will include recognition of risks and responding to concerns.
- Inform of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.

5.4 Parents and carers

The Oaks Academy will:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people.
- Ensure provision of resources, support and advice.
- Ensure provision and adherence to online safety policies and other policies of relevance.
- Advise of how and when to raise concerns.
- Provide details of all relevant contacts (for example, the DSL).

6. Cultivating a safe environment

“All staff should be aware of indicators, which may signal that children are at risk from, or are involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in well-being, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs” (DfE, 2019).

Children should be educated in an age-appropriate way around:

How to evaluate what they see online
How to recognise techniques for persuasion
Their online behaviour
How to identify online risks
How and when to seek support

6.1 Evaluate: How to evaluate what they see online

This will enable *students* to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

The Oaks Academy will help students to consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

6.2 Recognise: How to recognise techniques used for persuasion

This will enable students to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

The Oaks Academy will help students to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that industry use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.

6.3 Online Behaviour

This will enable students to understand what acceptable and unacceptable online behaviour looks like. The Oaks Academy will teach students that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. The Oaks Academy will also teach students to recognise unacceptable behaviour in others.

The Oaks Academy will help students to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online; and
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

6.4 Identify: How to identity online risks

This will enable *students* to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help *students* assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

The Oaks Academy will help students to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.

- Discussing when risk taking can be positive and negative.
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
- Discussing the risks versus the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

6.5 How and when to seek support

This will enable students to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

The Oaks Academy will help students by:

- Helping them to identify who trusted adults are.
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline and the Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education).
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

7. Responding to Online Safety Concerns

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for *The Oaks Academy* includes procedures to follow regarding online safety concerns.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies as per The Oaks Academy process.
- Always adhere to the academy safeguarding procedures and report to the DSL and/or Headteacher

8. Responding to Complaints

There are a number of sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer

- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk needs protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension).

It is also the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL and Head Teacher.

9. Monitoring and Filtering

Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. At the Oaks Academy, the DSL and the Digital safeguarding Lead work closely with our IT service provider. We use both Smoothwall and Impero systems and daily real time alerts are emailed to the Safeguarding team.

To understand and evaluate the changing needs and potential risks, we review our filtering and monitoring provision annually, or sooner if new technology is introduced, or there is a change in working practice. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), the Digital safeguarding Lead, the IT service provider and the school Safeguarding Governor. The review allows us to identify our current provision, any gaps, and the specific needs of our pupils and staff including;

- what our filtering system currently blocks or allows and why
- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements, for example PSHE curriculum
- what checks are currently taking place and how resulting actions are handled

Checks to our filtering provision are completed and recorded by our Digital Safeguarding Lead, as part of our filtering and monitoring review process.

10. Development of the Policy

This policy will be reviewed annually, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

References:

Department for Education (DfE) Keeping Children Safe in Education (KCSiE): Statutory guidance for schools and colleges. (September 2024)

Department for Education (DfE) Meeting digital and technology standards in schools (March 2023)

Department for Education (DfE) Teaching online safety in school: guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. (January 2023)

Department for Education (DfE) Working together to safeguard children. (July 2018)

Department for Education Cyberbullying: Advice for headteachers and school staff. (2014)

Safer Recruitment Consortium – Guidance for safer working practice for those working with children and young people in education settings (February 2022)

Children Act 1989
Children Act 2004
Communications Act 2003
Computer Misuse Act 1990
Criminal Justice and Courts Act 2015
Data Protection Act 1998
Data Protection Act 2018
Education Act 2011
Education and Inspections Act 2006
Freedom of Information Act 2000
Malicious Communications Act 1988