Online safety policy

September 2024

We empower | We respect | We care

Diverse Academies

Contents

1 Policy statement

1.1 Vision, mission and values

We are committed to creating a positive culture of online and offline behaviours, where all pupils feel valued and welcome, supporting student learning and success. Underpinning this policy is our commitment to empowerment, respect and care for all students and staff.

Our Trust mission is to ensure that all members of our community enjoy a positive, safe, and enriching online experience set within the specific context and ethos of each of our academies. We expect pupils and all stakeholders to contribute positively to the common good and uphold our expectations when online.

We aim to achieve and maintain positive and responsible online behaviours. We take a firm approach to all forms of online and offline bullying and discrimination across our academies through a commitment to fulfilling the Trust vision:

To inspire. To raise aspirations. To create brighter tomorrows.

1.2 Purpose and intent

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance.

This policy applies to all members of Diverse Academies. This includes staff and pupils, volunteers, parents/carers, visitors, and community users who have access to and are users of the Trust's digital technology systems.

All local systems adopted in our academies for managing online safety, including (but not exclusively) those incidents involving cyber-bullying and child-on-child sexual harassment and abuse, are centred on achieving a positive climate for learning and a respectful, secure culture for all children.

We recognise that poor online safety and dangerous or unhealthy online habits, especially if left unaddressed, can have adverse effects on individuals, both perpetrator and victim; it can create a barrier to learning and have serious consequences for social, emotional, and mental wellbeing.

We recognise that online safety is an essential element of safeguarding, and each academy duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

This policy supports academies in meeting statutory requirements as per the DfE guidance under the latest Keeping Children Safe in Education (2024), Working Together to Safeguard Children (2023) and non-statutory guidance, teaching online safety in academies (updated 2023).

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).

We recognise that effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda. We recognise that 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. Safeguarding children from online harm and abuse is everyone’s responsibility in our Trust.

We recognise the latest data from IWF (2021) that confirms that the vast majority of self-produced sexual imagery shared online is from girls in the 11-13 age range, but the fastest growing area is amongst 7–10-year-olds. This presents a particular challenge for both our primary and secondary phases.

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.

1. We believe that the internet and associated devices are an integral part of everyday life.

2. We affirm that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

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.

Current threats include the significant increase in Live Streaming (of sexual behaviours), coercion between minors, the sharing of nude and semi-nude images and the growth of chat sites. We commit to remaining aware of developments in social media and specific threats to childhood from the multitude of platforms.

2 Roles and responsibilities

It is imperative that a whole academy 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 policy will support a robust online safety ethos and ensure that academies are providing the best online safety provision they can.

The Trust board is responsible for ensuring that all pupils can access full time education and are safeguarded from harm or any sort of abuse. This is delegated to governors at a local level to provide appropriate support and challenge to senior leaders, ensuring that there is an appropriate and effective response to contextual concerns and risks, including online threats.

Senior leaders work together with the executive team to implement this, and other associated policies into practice in the academy ensuring every child can learn in a positive and supportive environment.

The following section outlines the online safety roles and responsibilities of all stakeholders across Diverse Academies.

2.1 Trustees and governors

Our Trustees and local academy committees ensure through delegation and robust strategic QA that the respective academy leadership team:

- upholds online safety as a safeguarding issue which is embedded across the whole academy's culture
- ensures that children are provided with a safe environment in which to learn and develop
- ensures that the academy has filters and monitoring systems in place
- ensures the academy has effective policies and training in place
- ensures that risk assessments are conducted on the effectiveness of filtering systems
- audits and evaluates online safety practice with the designated safeguarding lead and online safety lead
- ensures there are robust reporting channels via implementation and understanding of the safeguarding policy
- ensures that online checks are conducted and recorded on shortlisted and appointed personnel via the safer recruitment guidance in Part 3 KCSIE (Keeping Children Safe in Education)

2.2 Principals (with the support of the Executive Principal)

- delegate responsibility for ensuring the academy meets its duty in delivering effective online safety to designated staff including the Online Safety Lead, IT lead and Designated Safeguarding Lead.

  Through delegation, awareness training and regular QA they will:

- ensure children and young people are being appropriately taught about and know how to use the internet responsibly
- understand and quality assure the 'golden thread' that runs through Online Safety, from curriculum through to pupil voice, and the way the academy addresses child-on-child online abuse and behaviours
- clearly signpost online safety across the respective academy curriculum

- ensure the curriculum coverage is detailed in the local academy appendix
- 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, the online safety lead and computing lead.
- facilitate effective record keeping and the reporting and monitoring of all online safety concerns
- promote online safety and the adoption of a whole academy approach
- maintain their own training and learning needs, ensuring they are up to date with all matters relating to online safety
- ensure provision of robust filtering, monitoring, policies and practices as part of induction and ongoing training provision
- facilitate the designated safeguarding leads and the member of staff with responsibility for online safety completion of the NOS level 3 online safety accredited training
- provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or in response to online safety incidents arising
- ensure training includes recognition of risks and responses to concerns
- inform stakeholders about monitoring and filtering processes
- make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities
- advise about right resources to use
- ensure that all staff are aware of procedures to follow in recognising, responding to, and reporting online safety concerns
- ensure that the academy operates in accordance with the UK gov guidance ‘Meeting Digital and Technology Standards in Schools’
- ensure that our key online safety and safeguarding personnel work with the local county police POLIT (Paedophile Online Local Information Team), where suspected online abuse of minors has occurred
- ensure that all staff are committed to continuing professional development via NOS and the National College training modules in all areas concerning ‘online safety,’ GDPR and ‘acceptable use’
- ensure that key staff contacts are listed in the local academy appendix to this policy

2.3 Teachers and other staff

All members of Diverse Academies staff (teaching and non-teaching) have a responsibility to protect children online. This includes all members of staff who work at the academies - executive principal, principal, senior leaders, teachers, supply teachers, work-experience staff, office staff, nurses, caretakers, cleaners, etc. All staff must always act following their own professional boundaries, upholding professional behaviour and conduct at all times.

All staff need to:

- be aware of and adhere to all academy policies which support online safety and safeguarding
- contribute to policy development and review
- support in the ownership of, and responsibility for, the security of systems and the data accessed
- model good practice and appropriate behaviours when using technology – both in school and outside
- know the process for making referrals and reporting concerns
- know how to recognise, respond to, and report signs of online abuse and harm
- receive child protection awareness updates on online threats and safeguarding
- complete the National College Online Safety module as part of Trust mandatory training
- always act in the best interests of the child
- be responsible for their own continuing professional development in online safety
- understand that using My Concern to record safeguarding disclosures, necessitates a high standard of language, and objective reporting

2.4 Children and young people

With respect to online safety in our academies, children need to:

- know who the DSL (Designated Safeguarding Lead) and online safety lead teacher are
- engage in age-appropriate online safety education opportunities
- contribute to local academy policy and curriculum development and review
- read and adhere to local academy online safety policy appendices
- respect the feelings of others, both off and online
- take responsibility for keeping themselves and others safe online
- know where and how to find help with any online incidents or concerns
- know how, when, and where to report concerns and when to seek help from a trusted adult

2.5 Parents and Carers

We are committed to enabling parents and carers to understand the risks that children face online to protect them from online dangers. Parents should be encouraged via communication from respective academies to:

- read and adhere to all relevant policies
- be responsible when taking photos/using technology at academy events
- know who their child's academy DSL is
- know how to report online issues to the academy in the first instance
- support online safety approaches and education provision for their child(ren)
- be a role model for safe and appropriate behaviour
- identify changes in their child(ren's) behaviour that could indicate they are at risk of online harm or abuse

3 Benefits of the policy

Every child will be safe and free from bullying and discrimination, enabling them to learn and thrive in orderly, respectful, and purposeful learning environment leading to positive outcomes. All academies will have a school culture which celebrates positive learning and acknowledges respectful relationships at all levels.

4 Education and training

Effective online safety provision and promotion of the welfare of children and young people rely upon constructive relationships that enable 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. We follow the principles outlined in the non-statutory guidance 'Teaching Online safety in Schools, Jan 2023'.

Diverse Academies is committed to the importance of educating young people on the harmful effects of online behaviours relating to child-on-child sexual abuse and harassment. The policy statement should be read in conjunction with our approach to this emerging national agenda, the guidance found in Part 5 KCSIE, and the online resource found via our safeguarding partner, MyConcern: www.myconcern.co.uk/blog/peer-on-peer-abuse-in-schools-and-colleges

To further staff knowledge around online safety and to provide a wealth of curriculum resources across the phases, Diverse Academies remains committed to a partnership with the National College. Within the platform is access to National Online Safety (NOS) resources via #WakeUpWednesday.

https://nationalcollege.com

The support offered by NOS ensures online safety has a strong emphasis around training a competent workforce through knowledge of up-to-date policies and procedures, keeping ahead of the ever-changing online world, provision of webinars and accredited courses for staff at all levels.

We may also access resources, advice, and information from the IWF (Internet watch Foundation) when a concern or disclosure relates to suspected online sexual abuse.

Diverse Academies promotes and expects robust governance arrangements and collaborative practices.

In accordance with KCSIE 2024, our governors and staff receive specific training around understanding the purpose of filtering and monitoring, and what systems we have in place. See section 8.

Our staff recognise that online risks usually fall under one of three 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 frauds, bullying or harassing another child. They might create and upload inappropriate material or supply misleading information or advice.

4.1 Curriculum

Each academy has a bespoke, relevant curriculum offer around online safety. Details are outlined in the respective local academy online safety policy appendix.

We ensure each pupil receives education on safe and responsible use of and access to the internet through respective IT and wider PD (Personal Development) curriculum content, including online safety in personal, social, health and economic (PSHE) education, relationships and sex education (RSE), and information computer technology studies (ICT).

Diverse Academies will aim to equip children and young people for digital life.

Staff will promote safe and responsible internet use through teaching covering aspects of:

Age restrictions

- explaining that age verification exists and why some sites require a user to verify their age, for example, online gambling and purchasing of certain age restricted materials such as alcohol
- explaining why age restrictions exist, for example, to provide a warning that the site may contain disturbing material that is unsuitable for younger viewers
- helping pupils to understand how this content can be damaging to under-age consumers
- explaining what the age of digital consent means - the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations

How content can be used and shared

- what happens to information, comments or images that are put online.
- what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications
- how cookies work
- how content can be shared, tagged, and traced
- how difficult it is to remove something a user wishes they had not shared.
- the risk of identity theft or targeted approach from fraudsters using information shared online
- ensuring pupils understand what is illegal online, for example:

  youth-produced sexual imagery (sexting)

  sharing illegal content such as extreme pornography or terrorist content

  the illegality of possession, creating or sharing any explicit images of a child even if created by a child

Disinformation, misinformation, and hoaxes

Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.

Teaching may include:

- disinformation and why individuals or groups choose to share false information to deliberately deceive
- misinformation and being aware that false and misleading information can be shared inadvertently
- misinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs (including revenge porn)
- online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons
- explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online
- how to measure and check authenticity online
- the potential consequences of sharing information that may not be true

Fake websites and scam emails

Fake websites and scam emails are used to extort data, money, images, and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or another gain.

Teaching may include:

- how to look out for fake URLs and websites
- ensuring pupils understand what secure markings on websites are and how to assess the sources of emails
- explaining the risks of entering information to a website which is not secure
- what to do if harmed, targeted, or groomed as a result of interacting with a fake website or scam email
- who to go to and the range of support that is available
- explaining the risk of ‘too good to be true’ online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist

Fraud (online)

Fraud can take place online and can have serious consequences for individuals and organisations.

Teaching may include:

- what identity fraud, scams and phishing are
- explaining that online fraud can be highly sophisticated and that anyone can be a victim
- how to protect yourself and others against different types of online fraud
- how to identify ‘money mule’ schemes and recruiters
- the risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal
- the risk of sharing personal information that could be used by fraudsters
- explaining that children are sometimes targeted to access adults’ data, for example, passing on their parent or carer’s bank details, date of birth or national insurance number
- what good companies will and will not do when it comes to personal details, for example, a bank will never ask you to share a password or move money into a new account
- how to report fraud, phishing attempts, suspicious websites, and adverts

Password phishing

Password phishing is the process by which people try to find out your passwords so they can access protected content.

Teaching may include:

- why passwords are important, how to keep them safe and that others may try to trick you to reveal them
- explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords
- the importance of online security to protect against viruses (such as keylogging) that are designed to access, steal, or copy passwords.
- what to do when a password is compromised or thought to be compromised

Personal data

Online platforms and search engines gather personal data. This is often referred to as ‘harvesting’ or ‘farming.’

Teaching may include:

- how cookies work
- how data is farmed from sources which look neutral, for example, websites that look like games or surveys that can gather lots of data about individuals
- how, and why, personal data is shared by online companies, for example, data being resold for targeted marketing by email and text (spam)
- how pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential
- the rights children have regarding their data, including protections for children under the General Data Protection Regulations (GDPR)
- how to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time

Persuasive design

Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.

Teaching may include:

- explaining that most games and platforms are businesses designed to make money - their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue.
- how designers use notifications to pull users back online

Privacy settings

All devices, websites, apps, and other online services come with privacy setting that can be used to control what is shared.

Teaching may include:

- how to find information about privacy setting on various sites, apps, devices, and platforms
- explaining that privacy settings have limitations, for example, they will not prevent someone posting something inappropriate

Targeting of online content (including on social media and search engines)

Much of the information seen online is a result of some form of targeting.

Teaching may include:

- how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts
- how the targeting is done, for example, software which monitors online behaviour (sites they have visited in the past, people who they are friends with) to target adverts thought to be relevant to the individual user
- the concept of clickbait and how companies can use it to draw people onto their sites and services

We support learners' understanding based on age and ability through:

- 'Acceptable Use' posters in all rooms with internet access
- informing all learners of monitoring and filtering that is in place
- implementing peer education strategies
- providing continuous training and education as part of their transition across key stages
- using alternative, complementary support where needed
- seeking learner voice.

4.2 Vulnerable learners

Vulnerable children who need our help the most are not only missing opportunities to flourish online but are often experiencing the very worst that the online world can be.

We recognise that some learners are more vulnerable due to a range of factors. Those children may:

- receive statutory care or support
- have Special Educational Needs and Disabilities
- have experienced specific personal harm
- have a disability, be experiencing ill-health, or developmental difficulties
- live in households or families with characteristics or locations that indicate higher potential likelihood of current and future harm
- live in households where domestic abuse, parental substance abuse or mental health issues are present
- be vulnerable or of concern by virtue of their identity or nationality
- be at risk in relation to activity or institutions outside the home
- be a Young Carer

We will ensure the effective and safe provision of tailored online safety education for such pupils on a bespoke package, which augments the general academy offer.

We will seek input and advice from specialist staff, as necessary. For example, through our formal, professional relationship with National Online Safety (NOS) and the National College.

5 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 academies, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a notable 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).
The online world is increasingly used as a platform for the above.

Children in will be educated in an age-appropriate way about:

- 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

5.1 Evaluate – how to evaluate what pupils see online

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

Diverse Academies will help students/pupils to consider questions including (but not exclusively):

- 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?

5.2 Recognise – How to recognise techniques used for persuasion

This will enable pupils 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.

We help pupils to recognise:

- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation)
- techniques that companies 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

5.3 Online behaviour expectations

We expect that this section is read in conjunction with the Trust's Behaviour and Anti-Bullying policies.

This will enable staff to educate our pupils in understanding what acceptable and unacceptable online behaviour looks like. We teach children that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. We also teach them to recognise unacceptable behaviour in others.

We help pupils 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
- 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.

5.4 Identify – How to identity online risks

This will enable our staff to educate students/pupils in identifying possible online risks and make informed decisions about how to act. The focus is to help our children assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We help children 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
- 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?

5.4.1 Online radicalisation

We recognise that children, young people, and adult learners are at risk of accessing inappropriate and harmful extremist content online. This could include downloading or sharing terrorist material, which could be a criminal act.

The internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals.

Our teaching will include:

- how to recognise extremist behaviour and content online
- understanding actions which could be identified as criminal activity
- exploring techniques used for persuasion
- knowing how to access support from trusted individuals and organisations

We have a have a responsibility under the Prevent duty which includes building our students' resilience to extremism and ensuring staff are adequately trained to spot the signs of radicalisation.

5.4.2 Fake profiles

We recognise that not everyone online is who they say they are.

Teaching will include:

- explaining that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts)
- how to look out for fake profiles, for example:

  profile pictures that do not like right

  accounts with no followers or thousands of followers

  a public figure who does not have a verified account

5.4.3 Grooming

As part of our wider safeguarding duty, we expect designated staff and pupils in our academies to know about the different types of grooming and motivations for it, for example:

- radicalisation
- child sexual abuse and exploitation
- gangs (county lines)
- financial exploitation (money mules)

Teaching will include:

- boundaries in friendships with peers, families and with others
- the key indicators of grooming behaviour
- explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult
- how and where to report it both in school, for safeguarding and personal support, and to the police

5.4.4 Live streaming

We recognise that live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and watching it.

Teaching will include:

- explaining the risks of carrying out live streaming such as the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent
- that online behaviours should mirror offline behaviours and considering any live stream in that context - pupils should not feel pressured to do something online that they would not do offline
- explaining the risk of watching videos that are being live streamed, for example, there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance
- explaining the risk of grooming

5.4.5 Pornography

We understand and communicate that sexually explicit material presents a distorted picture of sexual behaviours. The teaching of this aspect of online safety is in conjunction with our wider safeguarding duty.

Teaching will include that:

- pornography is not an accurate portrayal of adult sexual relationships
- viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour
- that not all people featured in pornographic material are doing so willingly, such as revenge porn or people trafficked into sex work

This content is covered as part of the relationships and sex education core content (secondary).

5.4.6 Unsafe communication

Our pupils should know different strategies for staying safe when communicating with others, especially people they do not know or have never met.

Teaching will include:

- explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with
- identifying indicators or risk and unsafe communications
- identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before

- explaining about consent online and supporting pupils to develop strategies to confidently say “no” to both friends and strangers online

5.5 How and when to seek support

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

Diverse Academies will:

- help them to identify who trusted adults are
- look at the different ways to access support from police, the National Crime Agency’s Click CEOP reporting service for children, Internet Watch Foundation (IWF), National Online Safety, and organisations, such as Childline. The policy links to the wider Diverse Academies Trust policies and processes around reporting of safeguarding and child protection incidents and concerns to academy staff (see the current iteration of Keeping Children Safe in Education)
- help them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported

6 Responding to online safety concerns

Any concern that children and young people may be at risk of harm or abuse must immediately be reported.

The DSL takes the lead responsibility for online safety concerns, which are initially recorded and actioned in My Concern. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns.

Remember:

- child welfare is the principal concern – the best interests of children always take precedence over GDPR and any other restriction that may present itself
- if there is any immediate danger, contact the police on 999
- refer to all agencies as per Diverse Academies local safeguarding processes.
- always adhere to local safeguarding procedures and report to the DSL and principal within each academy – who will then act

7 Responding to complaints

There are several 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).

8 Monitoring, filtering, and compliance

In adhering to the guidance on filtering and monitoring in KCSIE the Trust uses the following:

,

SENSO

Each secondary academy has additional monitoring called Senso. Senso is a cloud-based solution that allows us to monitor and manage all student accessible Microsoft Windows computers throughout the network from a centralised web portal in real time.

DSLs (Designated Safeguarding Leads) may use this to view alerts for safeguarding violations and review and action the critical and urgent alerts. SENSO provides an overview of all violations across an academy or across the Trust. Staff can monitor and manage their classes online usage via this platform.

Watchguard

All pupils (and staff) who use our network to access the internet, are doing so through the Watchguard filtering and monitoring system. Our academies, in conjunction with the central Trust IT Team, manage the level of filtering required in each setting.

Monitoring Requirements	Analysing incident logs Checking planning for online safety lessons Student, pupils, parents, and carers questionnaires Evaluations
Monitoring Method	Watchguard and SENSO My Concern/safeguarding audit process
Monitoring Prepared by	DSL and/or academy online safety lead
Monitoring Presented to	Principal, executive principal and LAC (Local Academy Committees)
Frequency of Reporting	Full termly to LAC/annually to trust via audit.

9 The Online Safety Bill 2023

The Act is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms.

We always adhere to the online safety section of Keeping Children Safe in Education and take into consideration the detail in the Online Safety Act. We encourage our staff and parents to familiarise themselves with the key details in the Act using this hyperlink.

The Bill primarily protects children, by imposing a duty on user-to-user service providers to:

- remove harmful content or ensure that it does not appear in the first place
- enforce age limits and age-checking measures
- ensure risks and dangers to children's safety are more transparent, including publishing risk assessments

Any platforms that are likely to be accessed by children will now have a duty of care, which means the providers must take steps to protect children and young people from accessing content that is illegal and harmful. Some content, while not illegal, may be harmful or age-inappropriate for children.

Diverse Academies are alert to the impending legal guidance outlined in the Online Safety Act. For our academies, the safeguarding duties will remain the same. The Bill will not remove our responsibility or mean safeguarding children and young people online is put into the hands of third parties.

We will review all relevant policies and operational procedures in light of feedback and advice resulting from the OFCOM: Protecting Children from Harms Online consultation, May 2024.

10 Further sources of information

We follow the principles outlined in the guidance ‘Meeting digital and technology standards in schools and colleges, March 2023’

In addition to the above, the links below, to relevant government guidance and a range of national organisations can offer support to parents and schools.

Related guidance is available on:

- relationships and sex education (RSE) and health education
- national curriculum in England computing programmes of study
- national curriculum in England citizenship programmes of study

Support and resources are also available from:

- the CEOP Thinkuknow Programme
- the NCA’s Click CEOP
- National Centre for Computing Education (NCCE)
- UK Council for Internet Safety
- Education for a Connected World

Our academies can also get advice from national organisations such as:

- Anti-Bullying Alliance
- Association for Citizenship Teaching
- Childnet
- The Diana Award
- DotCom Charity
- Hopes and Streams
- Internet Matters
- Internet Watch Foundation
- NSPCC learning
- PSHE Association
- SWGfL

- UK Safer Internet Centre

Our parents may also access the following national organisations for support:

- Internet Matters
- NSPCC
- Parent Zone

Our pupils may access the following national organisations for support:

- BBC Own It
- Childline

11 Disclaimer and review

Every effort has been made to ensure that the information contained within this policy is up to date and reflective of the latest legislative and statutory guidance. The online world is fast changing, and we recognise that areas of policy may need to be adapted and amended to reflect this. If errors are brought to our attention, we will correct them as soon as is practical.

This policy will be reviewed at least biennially in the summer term to reflect legislative changes or developments, to ensure its continuing relevance.