Dane Court Grammar School

Online Safety Policy

Date policy last reviewed: August 2025

Date policy next reviewed: August 2026.

Signed by:

Headteacher Date: 29/08/2025

Chair of governors Date:

Coastal Academies Trust (CAT)

1. CAT SAFEGUARDING STATEMENT

CAT is wholly committed to ensuring that all children and young people are cared for in a safe, nurturing and secure environment in our academies. We are fully committed to safeguarding and promoting the welfare of all the pupils and staff within the academy trust and expect all staff and volunteers to share this commitment. To fulfil this commitment we have robust systems in place for:

- Policy and procedures
- Safe recruitment of staff and volunteers
- CAT responsibilities
- Training

2. Policy and procedure

The online safety policy is reviewed and agreed on an annual basis to ensure that key messages from legislation and guidance are embedded within all of our academies. Policy and procedures are developed using key Government guidance.

Additional support and challenge is made to ensure other safeguarding policies and procedures are effective such as Safeguarding and Child Protection, Anti Bullying, Codes of Conduct, Pupil Behaviour and Attendance.

CAT expects that each academy will follow the guidance and child protection procedures provided by their Local Authority children's services departments.

3. Safe recruitment of staff and volunteers

Safer recruitment is an important part of safeguarding children and is the first step to safeguarding and promoting the welfare of children in education. CAT views it is vital that there is a culture of safe recruitment and has adopted recruitment procedures that will deter, reject and identify people who might be unsuitable to work with children and young people.

Each academy has a Safer Recruitment Policy to ensure that the recruitment and selection processes outlined:

- are robust and meet the requirements of Keeping Children Safe in Education September 2023
- have relevant vetting and checking procedures
- include a robust induction
- provide an ongoing training infrastructure

The policy outlines the steps that academies within our trust will take to ensure those employed in our academies are safe to work with children and young people and its main purpose is:

- to prevent unsuitable people working within our schools
- to attract the best possible candidates to work in our schools
- to create and maintain a safe workforce

Each school maintains a single central record to provide reassurance that all staff and volunteers are recruited safely. The trust undertakes annual peer to peer checks across the trust which include providing challenge and support to ensure the SCR is compliant.

4. CAT responsibilities

CAT is committed to the following core safeguarding principles;

- The Trust's responsibility to safeguard and promote the welfare of children is of paramount importance.
- All children, regardless of age, gender, ability, culture, race, language, religion or sexual identity, have equal rights to protection.
- Children who are safe and feel safe are better equipped to learn.
- The Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, Governors and Directors to share this commitment.
- All staff, volunteers, Governors and Directors have an equal responsibility to act on any suspicion or disclosure that may suggest a child is at risk of harm at home, in the community or in an academy.
- If, at any point, there is a risk of immediate serious harm to a child a referral will be made to Children's Social Care immediately.
- All staff members will maintain an attitude of 'It could happen here' where safeguarding is concerned. When concerned about the welfare of a child, staff members are to always act in the interests of the child.
- Students and staff involved in child protection issues will receive appropriate support.
- Policies will be reviewed at least annually unless an incident or new legislation or guidance suggests the need for an interim review.

5. Training

CAT ensures that its academies comply with training requirements as defined in Keeping Children Safe in Education;

- All school staff must undergo safeguarding and child protection training at induction and a signed record will be kept of those who have attended. This training should be updated "regularly" and a record will be kept of those who have attended.
- Safeguarding training during induction should give staff an awareness of the school's safeguarding systems. Induction training should also cover:
- The child protection policy
- The staff behaviour policy/code of conduct (training should cover the school's whistleblowing procedures)
- The role of the designated safeguarding lead (DSL)
- The DSL and any deputy DSLs should undergo training that provides them with the knowledge and skills needed to perform the role. This training should be updated every two years.
- The DSL should undertake training on the government's anti-radicalisation strategy, Prevent. All staff, volunteers and Governors receive Prevent training.
- The knowledge and skills of the DSL and deputies should be updated "at regular intervals".
- The DSL and Deputy DSLs across the trust meet as a group during the academic year to share practice, updates and feedback on peer to peer to reviews, to ensure compliance and consistency of approach across the trust
- Safer recruitment training is completed for required staff and Chair of Governors.
- Our academies are additionally required to ensure all staff, volunteers and Governors have opportunities to explore learning in relation to female genital mutilation, managing allegations and online safety.

Contents:

Statement of intent

Dane Court understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, for example:
    - Pornography.
    - Racism.
    - Misogyny.
    - Self-harm.
    - Suicide.
    - Discrimination.
    - Radicalisation.
    - Extremism.
    - Misinformation.
    - Disinformation, including fake news.
    - Conspiracy theories.
- **Contact**: Being subjected to harmful online interaction with other users, for example:
    - Peer to peer pressure.
    - Commercial advertising.
    - Adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.

- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, for example:
    - Making, sending and receiving explicit messages.
    - Consensual and non-consensual sharing of nudes and semi-nudes.
    - Sharing of pornography.
    - Sharing other explicit images.
    - Online bullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff will revolve around these areas of risk.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

6. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy

- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy
- Safe Use of AI Policy

7. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.

- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the cyber-security recommendations.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school and working with the Safeguarding team to ensure training is appropriate.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Holding an annual review with SOTA to ensure that they are abreast of changes and/or concerns.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Providing specialist knowledge in relation to filtering system management, e.g. the content and websites pupils should and should not be able to access.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

SOTA/IT Technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.
- Providing specialist support in relation to the implementation of filtering and monitoring software.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

We ask that our parents/carers are responsible for:

- Reading our Acceptable Use of technology policies and encourage their child(ren) to adhere to them.
- Supporting our online safety approaches by discussing online safety issues with their child(ren) and reinforcing appropriate and safe online behaviours at home.
- Role modelling safe and appropriate use of technology and social media and abiding by the home-school agreement and acceptable use of technology policies.
- Seeking help and support from the school or other appropriate agencies if they or their child(ren) encounter online issues.
- Contributing to the development of our online safety policies.
- Using our systems, such as learning platforms and other IT resources, safely and appropriately.
- Taking responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their child(ren) access and use at home.

8. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive training regarding online safety information and any changes to online safety guidance or legislation through staff meetings/briefings.
- Online safety is integrated into learning throughout the curriculum
- Assemblies delivered to students which cover online safety.
- Nominated member of the Safeguarding team has a specific focus on online safety.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents/carers to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby

it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and/or SOTA, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

9. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

10. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy and involve external agencies if/where appropriate.

11. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

12. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL, along with the school's mental health lead, will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

13. Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

14. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means

overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

15. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

16. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE

- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online will always be considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

17. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers/chrome books
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

18. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom. Mobile phones are expected to be out of sight and switched off whilst on the school site. They may be confiscated if school rules are not adhered to.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

19. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child(ren) to ensure their child(ren) understand(s) the document and the implications of not following it.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents/carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental/Carer awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters/email communication
- Online resources

20. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

21. Filtering and monitoring online activity

Filtering system: Smoothwall

Monitoring system: Senso

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and SOTA will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems will be scaled appropriately to meet the safeguarding needs of all pupils. SOTA will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, SOTA and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by SOTA. Reports of

inappropriate websites or materials will be made by members of the school community to SOTA immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and SOTA, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.

Filtering:

- Smoothwall is a member of Internet Watch Foundation (IWF). Leaders should check to ensure this is the case.

- Dane Court/SOTA have signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) Leaders should check to ensure this is the case.

- Smoothwall is blocking access to illegal content including child sexual abuse material (CSAM).

- Smoothwall blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

- We filter internet use on all school owned, or provided, internet enabled devices and networks.

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

- We work with our ISP/Smoothwall and our staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements. Staff are encouraged to ask IT to restrict access to any site they deem inappropriate. The DSL/Safeguarding team if a student/staff member is asking for a site to be unblocked.

- If there is failure in the software or abuse of the system, for example if students or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to alert a DSL.

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

- Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), the police (either via 101 or 999 if an emergency or NCA-CEOP) or Children's Social Care.

- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

Monitoring

Dane Court has consulted the UK Safer Internet Centre guidance and the DfE filtering and monitoring standards to inform Filtering and Monitoring approaches within the school.

No monitoring system can be 100% effective, but the following measures are in place to reduce risk:

- We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:
    - School owned devices will be monitored by the monitoring software, Senso. For school owned IPADs, the class teacher will use the equivalent monitoring app.
    - All staff members should also physically monitor the use of student devices, circulating the classroom and ensuring that any student (typically only applicable to sixth form) who is using their own device is connected to the BYOD Wifi. All other students should be using a school owned device (unless in exceptional pre-agreed circumstances where the aforementioned procedure must be followed).
    - Staff reserve the right to ask that a pupil uses a student owned device in their classroom if they are worried that a pupil is at risk of harm. This should additionally be communicated with the DSL/Safeguarding team.
    - Senso will continue to track the use of school owned devices beyond the school setting. Pupils should be aware that this is the case, but that staff are not expected to be monitoring this outside of school hours. This is the responsibility of parents/carers/guardians, but the school will act accordingly if any malpractice/risk of harm is detected.

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
- Where the concern relates to pupils, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.
- Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behaviour/allegations policy.
- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, the Police via 101 or NCA-CEOP , the LADO or Children's Social Care.

22. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems which should not be shared with anyone. Pupils will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. SOTA will be responsible for generating regular password resets.

Users will inform SOTA if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber-security Policy.

23. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. SOTA will work with the DSL to ensure that pupils/staff are aware:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

24. Generative artificial intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use of AI tools comply with wider statutory obligations, including those outlined in KCSIE. The DSL/SLT may choose to block the use of AI and will review its use on a case by case basis.

The school will carry out an AI Risk Assessment, which includes plans for mitigating against unauthorised use cases.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

For any use of AI, the school will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).
- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's generative AI product safety expectations and filtering and monitoring standards.

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

The school will introduce a comprehensive Safe Use of AI Policy that clearly defines how AI technologies will be utilised responsibly and securely. This policy will outline the potential risks associated with misuse, as well as the safeguarding measures the school will implement to ensure the safe and ethical application of AI tools

25. Social Media

The use of social media by staff and pupils will be managed in line with the school's policy.

1. **Expectations**
   - Dane Court believes everyone should be treated with the school's values of being caring, open minded and principled in mind. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.

   - All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

   - We will restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems; further information on how this is achieved in addressed in our child protection policy.

   - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary action.

   - The use of social media or apps, for example as a formal remote learning platform or education tool will be robustly risk assessed by the DSL and/or headteacher prior to use

with learners. Any use will take place in accordance with our existing policies, for example, child protection, staff/learner behaviour acceptable use policies.

- Concerns regarding the online conduct of any member of the Dane Court community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff behaviour/code of conduct, Acceptable Use Policies, and child protection policies.

0. **Staff use of social media**

- The use of social media during school hours for personal use is not appropriate for staff.

- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct/behaviour policy and/or acceptable use of technology policy.

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

a) Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.

- Members of staff are encouraged not to identify themselves as employees of Dane Court on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.

- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.

- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

b) Communicating with pupils and their families

- Staff will not use any personal social media accounts to contact pupils or their family members.

- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media accounts.

- Any communication from pupils and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and/or the headteacher.

- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard pupils, members of staff and the setting.

- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

0. Official use of social media

- Dane Court has official social media channels.

- The official use of social media sites by Dane Court only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the headteacher prior to use.

- Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
    - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.

- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Parents and carers will be informed of any official social media use with pupils any official social media activity involving pupils will be moderated if possible and written parental consent will be obtained as required.

- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read and understand our Acceptable Use Policy.
    - Where they are running official accounts, sign our social media Acceptable Use Policy.
    - Be aware they are an ambassador for the school.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.

- Not engage with any private or direct messaging with current or past pupils or their family members.
- Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

0. Pupils' use of social media

- The use of social media during school hours for personal use **is not** permitted for pupils.

- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another pupils, could have repercussions for the orderly running of the school when the pupils is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.

- Dane Court will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies such as RSE and Computing.

- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions.

- Pupils will be advised:
  - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
  - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.

- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

- Any concerns regarding pupils' use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.

- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.

- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.

- Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

26. The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

27. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. The use of these devices should be used in line with the school's acceptable use policies.

Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

28. Mobile Phones

a) Mobile and Smart Technology

- Our mobile and smart technology policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

b) Safe use of mobile and smart technology expectations

- Our school recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
  - take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.

- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes changing rooms, toilets and swimming pools. From September 2024, pupils are permitted to have their mobile phones in their bags and **switched off**, but they **must not be seen or used <u>at all</u>** on the school premises. This is with the exception of Sixth Form, who only have permission to use their devices in the designated Sixth Form area, as outlined by the Sixth Form team.

- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child

protection policies.

- All members of our community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

0. School provided mobile phones and devices

- In the event that a member of staff is required to use a school owned device (school laptop, school phone for trips etc), they will be issued with a work phone number in addition to their work email address, where contact with pupils or parents/carers is required.

- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy. This must discussed with the DSL/headteacher.

- School provided mobile phones and/or devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff and/or pupils/students where appropriate.

- School provided mobile phones and/or devices will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies. Amend as appropriate.

- Where staff and/or pupils/students are using school provided mobile phones and/or devices, they should be aware that activity may be monitored for safeguarding reasons and to ensure policy compliance.

0. Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security, staff behaviour/code of conduct and Acceptable Use Policies.

- Staff will be advised to:
    - Keep personal mobile and smart technology devices in a safe and secure place during lesson time.
    - Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
    - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - Not use personal mobile or smart technology devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own mobile and smart technology devices for contacting pupils or parents and carers.
    - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and/or headteacher.

- Staff will only use school provided equipment (not personal devices):
    - to take photos or videos of pupils/students in line with our image use policy.
    - to work directly with pupils/students during lessons/educational activities.
    - to communicate with parents/carers.

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct, child protection and/or allegations policy.

- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our staff behaviour/allegations/child protection policy.

0. Pupils/students use of mobile and smart technology

Dane Court's policy has been informed by government guidance and non-statutory guidance including: '<u>Mobile Phones in Schools</u> as part of their decision making.

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.

- Safe and appropriate use of mobile and smart technology will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection, behaviour and relevant specific curriculum policies, for example, RSE and Computing.

- Personal mobile or smart technology devices are not permitted on site by pupils with the exception of Sixth Form students, who are only permitted to do so in the designated Sixth Form area, as pre determined by the Head of Sixth and Sixth form team.
    - Pupils/students are not permitted to use personal mobile or smart devices whilst on the school site. Where these are required, for example for safety reasons when children/young people are transporting to and from school, devices should be turned off/placed on silent and kept in their bag unless directed otherwise by the SLT.
    - Personal mobile or smart devices will not be used by pupils/students during lessons or formal educational time, unless in exceptional circumstances as part of an approved and directed curriculum-based activity with consent from a member of the SLT.
    - The use of personal mobile or smart devices for a specific education purpose does not mean that blanket use is permitted.

- Staff will only allow pupils to use personal mobile or smart devices as part of an educational activity, following a risk assessment, with approval from the Leadership Team.

- Dane Court expects pupils' personal mobile or smart technology devices to be kept safe and secure when on site. This means:
  - kept out of sight during lessons and while moving between lessons. They should be switched off and kept as securely as possible.

- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to ask their Head of Year or make contact with the office.
  - Parents/carers are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

- If a pupil requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.
  - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
  - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and/or their parents/carers before use is permitted.

- Where pupils' personal mobile or smart technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.

- Personal mobile or smart technology devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

0. Searching, screening and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

- Where there are any concerns regarding pupils' use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.

- Staff may confiscate a pupils' personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.

- Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers from the office. Where it is deemed appropriate a senior member of staff or member of SLT may need to speak to the parent/carer at greater length.

- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.

- If there is suspicion that data or files on a pupils' personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance. The headteacher or a member of staff authorised by the headteacher can carry out a search and examine any data or files on an electronic device confiscated as a result of a search, if there is good reason to do so. This would be where they have reasonable grounds for suspecting the device or content on the device poses a risk to staff and/or pupils/students, is prohibited, or identified in the school's behaviour policy for which a search can be made or is evidence in relation to an offence. The headteacher can authorise individual members of staff to search for specific items, or all items set out in the school's behaviour policy.

- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil electronic device that they reasonably suspect are likely to put a person at risk.

- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.

- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology device has revealed a safeguarding risk.

- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so. The DfE **'Searching, Screening and Confiscation'** guidance states (77 – 79)
    - In determining whether there is a 'good reason' to examine images, data or files, the headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
    - If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

0. Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that phones and smart technology do not disrupt the running of the school day.

- Appropriate information is available to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology device.

- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use personal mobile or smart technology device in accordance with our acceptable use of technology policy and other associated policies, including child protection.

- If visitors require access to personal mobile or smart technology device, for example when working with pupils as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.

- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

0. Responding to Online Risks and/or Policy Breaches

- All members of the community:
    - are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

- will be made aware of how the school will monitor policy compliance
- are expected to adopt a partnership with the school to resolve issues.

- If appropriate, after any investigations are completed, the DSL and leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- If we are unsure how to proceed with an incident or concern, the DSL or headteacher will seek advice from the local authority or other agency in accordance with our child protection policy.

- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL and/or headteacher will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

1. Concerns about pupil online behaviour and/or welfare

- Dane Court recognises that an initial disclosure to a trusted adult may only be the first incident reported, rather than representative of a singular incident and that trauma can impact memory, so children may not be able to recall all details or timeline of abuse. All staff will be aware certain children may face additional barriers to telling someone, for example because of their vulnerability, disability, sex, ethnicity, and/or sexual orientation.

- All concerns about pupils will be responded to and recorded in line with our child protection policy:
    - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
    - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

- Abuse that occurs online and/or offsite will not be dismissed or downplayed; concerns will be treated equally seriously and in line with relevant policies/procedures, for example anti-bullying, behaviour, child protection, online safety.

- Dane Court recognises that the law is in place to protect children and young people rather than criminalise them, and this will be explained in such a way to pupils that avoids alarming or distressing them.

- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

0. Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be managed in accordance with our allegations against staff policy/staff code of conduct/behaviour policy.

- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer

- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

0. Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.

- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

0. Procedures for responding to specific online concerns

1. Online child-on-child abuse

- Dane Court recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our child protection and behaviour policies.

- We recognise that online child-on-child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as 'sexting' or 'youth produced sexual imagery')
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
  - initiation/hazing type violence and rituals.

- Dane Court adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse and it will never be tolerated or dismissed as "just banter", "just having a laugh", "part of growing up" or "boys being boys"; this can lead to a culture of unacceptable behaviours and can create an unsafe environment for children and a

culture that normalises abuse, which can prevent children from coming forward to report it.

- Dane Court believes that all staff have a role to play in challenging inappropriate online behaviours between children. Staff recognise that some online child-on-child abuse issues may be affected by gender, age, ability and culture of those involved.

- Dane Court recognises that even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.

- Concerns about child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with pupils' and parents/carers; concerns will be recorded and responded to in line with existing appropriate policies, for example anti-bullying, acceptable use, behaviour and child protection policies.

- Dane Court want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child-on-child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Pupils who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

11.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Dane Court will follow the guidance outlined in Part Five of KCSIE.

- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.

- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.

- Dane Court recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.

- Dane Court recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services, and for things to move from platform to platform online.
- Dane Court will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

- Dane Court will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.

- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator, and any other children involved/impacted.

- The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children, adult students and staff and any actions that are required to protect them.
- Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the police.
- The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
- If content is contained on pupils' personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation']' advice.

- Following an immediate risk assessment, the school will:
  - provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
  - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
  - if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
  - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

- Dane Court recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Dane Court also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

11.1.2 Nude or semi-nude image sharing

- Dane Court recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
    - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
    - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
    - possesses nude and/or semi-nude imagery created by another person under the age of 18.

- When made aware of concerns regarding nude and/or semi-nude imagery ,Dane Court will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

- Dane Court will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.

- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
    - Report any concerns to the DSL immediately.
    - Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery, this will be immediately reported to the DSL.
    - Not delete the imagery or ask the child to delete it.
    - Not say or do anything to blame or shame any children involved.
    - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.

- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
  - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
  - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of pupils involved, including the possibility of carrying out relevant checks with other agencies.
  - a referral will be made to Children's Social Care and/or the police immediately if:
    - the incident involves an adult (over 18).
    - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
    - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
    - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
  - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
  - If DSLs are unsure how to proceed, advice will be sought from the local authority.
  - Store any devices securely:
    - If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
  - provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - implement sanctions where necessary and appropriate in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
  - consider the deletion of images in accordance with the UKCIS guidance.

        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
        - Pupils will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
    - review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. Where necessary, the DSL will consult the document 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request pupils to do so.

0. Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Dane Court

- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

0. Online child abuse and exploitation

- Dane Court recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection policy.

- Dane Court will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.

- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
    - store any devices containing evidence securely:
        - If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a pupil is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of pupils involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
    - Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/

- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police.

- We will ensure that the NCA-CEOP reporting tools are visible and available to pupils and other members of our community.

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.

- If members of the public or pupils at other schools or settings are believed to have been targeted, the DSL, will seek advice from the police and/or the Local Authority before sharing specific information to ensure that potential investigations are not compromised.

0. Child Sexual Abuse Material (CSAM)

- Dane Court will ensure that all members of the community are made aware of the possible consequences of accessing Child Sexual Abuse Material (CSAM), also known as Indecent Images of Children (IIOC), as appropriate. Any concerns related to consensual and non-consensual nude or semi-nude images sharing by children, will be responded to in line with section 11.1.2 of this policy.

- We will respond to concerns regarding CSAM on our equipment and/or personal equipment, even if access took place off site.

- We will seek to prevent accidental access to CSAM by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Local Authority.

- If made aware of concerns relating to CSAM, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.
    - lock/limit access and store any devices involved securely to prevent further viewing or deletion of evidence etc, until advice has been sought.

        - If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.

- If made aware that a member of staff or a pupil has been exposed to CSAM we will:
    - ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or to the police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by pupils.
    - report concerns as appropriate to parents and carers.

- If made aware that CSAM has been found/viewed on school provided networks/devices, we will:
    - ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.

- If made aware that a member of staff has viewed or is in possession of CSAM, we will:
    - quarantine any involved school provided devices/network access until police advice has been sought.
    - ensure that the headteacher is informed in line with our behaviour/managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police, in accordance with our behaviour/managing allegations against staff policy.

0. Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Dane Court and will be responded to in line with existing policies,

including child protection, anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police.

0. Online radicalisation and extremism

- As per section 7 of this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with our child protection, staff behaviour/code of conduct and/or allegations policies.

0. Cybercrime

- Dane Court recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.

- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

- Where there are concerns about 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with our child protection policy and other appropriate policies.

29. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is **August 2026**.

Any changes made to this policy are communicated to all members of the school community.

30. Useful links:

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- South West Grid for Learning (SWGfL): 360 Safe Self-Review tool for schools www.360safe.org.uk
- London Grid for Learning: https://lgfl.net/safeguarding
- Childnet: www.childnet.com

    - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
    - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.ceopeducation.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
    - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Internet Matters: www.internetmatters.org
- Childnet: www.childnet.com
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parents Protect: www.parentsprotect.co.uk
- NCA-CEOP Child and Parent Resources: www.ceopeducation.co.uk
- Parent Zone: https://parentzone.org.uk
- Get Safe Online: www.getsafeonline.org

Common Sense Media: www.commonsensemedia.org