Northease Manor School

Online Safety Policy

Frequency of review:	Annually, or whenever government updates require it			
Dates of previous review:	September 2025, September 2026			
Date of next formal review:	September 2027			
Linked policies/documents:	Anti-Bullying Policy Positive Behaviour Policy Child Protection and Safeguarding Policy			
	Name	Role	Signature	Date
Policy Owner	Martin Waite	Assistant Head – Behaviour and Engagement and DSL	Martin Waite	September 2026
Ratified by (governor)	Full Governing Body			September 2026

Contents

	Page no
1. Policy Aims	5
2. Policy Scope	5
2.1 Links with other policies and practices	6
3. Monitoring and Review	6
4. Roles and Responsibilities	6
4.1 The leadership and management team and governors	7
4.2 The Designated Safeguarding Lead	7
4.3 Members of staff	8
4.4 Staff who manage the technical environment	9
4.5 Learners	9
4.6 Parents	9
5. Education and Engagement Approaches	10
5.1 Education and engagement with learners	10
5.2 Vulnerable Learners	11
5.3 Training and Engagement with staff	12
6. Responding to Online Safety Incidents and Concerns	13
6.1 Concerns about Learner Welfare	13
6.2 Staff Misuse	14
7. Procedures for Responding to Specific Online Incidents or Concerns	14
7.1 Online Sexual Violence and Sexual Harassment between Children	14
7.2 Making or Sharing Nudes and Semi-Nudes (including AI-generated images)	15
7.3 Online Child Sexual Abuse and Exploitation including County Lines	16
7.4 Indecent Images of Children (IIOC)	17
7.5 Cyberbullying	18
7.6 Cybercrimes	18
7.7 Online Hate	19
7.8 Online Radicalisation and Extremism	19
8. Safer Use of Technology	20
8.1 Classroom Use	20
8.2 Managing Internet Access	20
8.3 Filtering and Monitoring	20
8.4 Managing Personal Data Online	21
8.5 Security and Management of Information Systems	21
8.5.1 Password policy	22
8.6 Managing the Safety of the Website	22
8.7 Publishing Images and Videos Online	22
8.8 Managing Email	22
8.9 Live Stream Lessons for Remote Learning	23
8.10 Management of Learning Platforms	25
8.11 Management of Applications (apps) used to Record Learners Progress	25
8.12 Generative Artificial Intelligence (AI)	26
9. Social Media	26

9.1 Expectations 26
9.2 Staff Personal Use of Social Media 27
9.3 Learners' Personal Use of Social Media 28
9.4 Official Use of Social Media 28
10. Use of Personal Devices and Mobile Phones 30
10.1 Expectations 30
10.2 Staff Use of Personal Devices and Mobile Phones 31
10.3 Learners' Use of Personal Devices and Mobile Phones 31
10.4 Visitors' Use of Personal Devices and Mobile Phones 32
10.5 Officially provided mobile phones and devices 32
11. Useful Links for Education Settings 33

Online Safety Policy

1. Policy Aims

- This online safety policy has been adapted by Northease Manor School, involving staff, learners and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education 2026, and the East Sussex Safeguarding Children Partnership procedures.

- The purpose of this online safety policy is to:
    - Safeguard and protect all members of our community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- We identify that the issues classified within online safety are considerable and ever evolving, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material, for example pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories
    - **Contact:** being subjected to harmful online interaction with other users or with generative AI applications that simulate this, for example peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them 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 images (including those generated using AI) and online bullying.
    - **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams and sextortion (online sexual coercion and extortion of children)

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf

of the setting (collectively referred to as “staff” in this policy) as well as learners, parents and carers.

- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to member of the school/academy.
- In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school. Action can only be taken over issues covered by the published Positive Behaviour Policy.

2.1 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Positive Behaviour policy
- Child protection and Safeguarding policy
- Curriculum policies, such as: ICT, Personal Social and Health Education (PSHE), and Relationships, Sex and Health Education (RSHE)
- Data security
- GDPR Policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; We will review this policy at least annually
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding Philippa Field will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Martin Waite (Assistant Head – Behaviour and Engagement), has lead responsibility for online safety and will liaise with key members of staff, for example the Operations and Facilities Manager and the ICT teacher.

    - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team and governors will:

- Understand that they have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Be responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to conduct their roles and train other colleagues, as relevant.
- Ensure that there is a system in place to allow for monitoring and support of those in school who conduct the internal online safety monitoring role.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies (including the staff code of conduct and/or acceptable use policies) and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the school's IT system and therefore have appropriate filtering and monitoring systems in place. They will have an awareness and understanding of the provisions in place and will collaborate with technical staff to monitor the safety and security of our systems and networks.
- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.
- Ensure that they regularly review the effectiveness of filters and monitoring systems at least once every academic year. The review will be carried out by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support, and will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations; a record of these checks will be kept; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that the DfE's filtering and monitoring standards for schools and colleges are being met this will be supported through using the checklist appended to this policy and making use of the government resource Plan technology for your school.
- Make use of the government guidance Generative AI: product safety expectations and Generative artificial intelligence in education, together with the DfE's online resources to help staff use AI safely

and effectively, to ensure the safe use of generative artificial intelligence within the school (see section 8.12).

- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.
- Ensure that all staff, including those who do not work directly with children, read and understand Part one of Keeping Children Safe in Education 2026, and that mechanisms are in place to help them understand and discharge their roles and responsibilities.
- Support the DSL and any deputies by ensuring they have the additional time, funding, training, resources and support they need to conduct the role effectively.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice, annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.
- Communicate with parents regarding the importance of children being safe online, the systems being used in school and information regarding what their children are being asked to do online by the school.
-

4.2 The Designated Safeguarding Lead (DSL) will:

- Hold the lead responsibility for online safety (including understanding the filtering and monitoring systems and processes in place), within their safeguarding role.
- Be an appropriate senior member of staff from the school leadership team.
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Collaborate with deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are conducted.
- Support the SLT member responsible for filtering and monitoring to review the effectiveness of filtering and monitoring at least once every academic year, ensuring that a record of these checks is kept.
- Attend relevant governing body meetings/groups.
- Report regularly to Governors/headteacher/senior leadership team.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input, including from pupils.

- Be responsible for receiving reports of online safety incidents and managing them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Consult with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Collaborate with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Ensure robust cover arrangements are in place for periods when the DSL is unavailable, so that online safety concerns are received, monitored and acted upon without delay (for example, through a confidential shared safeguarding inbox).

4.3 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Be aware that children can abuse other children online, including through abusive, harassing and misogynistic/misandrist messages, the non-consensual making or sharing of nudes or semi-nudes (including AI-generated or digitally altered images), especially around chat groups, and the sharing of abusive images and pornography with those who do not want to receive such content.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Read and understand Part one of Keeping Children Safe in Education 2026.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Understand that online safety is a core part of safeguarding.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reinforce the school's online safety messages when teaching lessons online

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures for example encryption and password protected systems to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Policies.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the Acceptable Use Policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- We will establish and embed a broad, relevant, and progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships, Sex and Health Education (RSHE), computing programmes of study, through our assembly and active tutorial programme.
    - Ensuring the curriculum builds on prior knowledge and is accessible for all pupils, including those with SEND and EAL.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Teaching learners about online harms such as sharing images, the prevalence of deepfakes and other AI-generated content, pornography and misogynistic influencers, and when and where to seek help.
- We will support learners to read and understand the Acceptable Use Policies in a way which suits their age and ability by:
    - Acting as good role models in their use of digital technologies, the internet and mobile devices.
    - Displaying age-appropriate acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology.
    - Implementing appropriate peer education approaches.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- We recognise that our learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. Online safety, is covered regularly within our active tutorial and assembly programme as well as regular visits from our police liaison officer.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff and governors on a regular basis, with at least annual updates.
    - This is achieved as part of existing safeguarding child protection training/updates, additional CPD training and through our online training package, Educare
    - This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, and the safe use of generative AI.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Ensure all new staff receive online safety training as part of their induction programme.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
        - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in our E-safety newsletters and letters.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.
    - Providing them with information about our approach to filtering and monitoring as well as information about the types of things that children will be doing online.

6. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, the making or sharing of nudes and semi-nudes (including AI-generated images), cyberbullying and illegal content.
- All members of the community will be directed to the DSL or Headteacher in such circumstances.
- All reports will be taken seriously and will be dealt with as soon as is practically possible.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Information about online safety concerns will be shared appropriately and in a timely way, in line with data protection laws (the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025) and the information sharing duty introduced by the Children's Wellbeing and Schools Act 2026. Fears about sharing information will not be allowed to stand in the way of the need to safeguard children.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, should be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
- Where there is suspicion that illegal activity has occurred contact the Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL (or deputies) will contact Sussex Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Learners' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputies) will record these issues on MyConcern, in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Sussex Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

6.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher in accordance with the allegations policy.
- For any allegations regarding a member of staff's online conduct a consultation will be sought with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

7. Procedures for Responding to Specific Online Incidents or Concerns

7.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood part 5 of Keeping Children Safe in Education 2026.
- We recognise that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos (including AI-generated or digitally altered images, sometimes described as 'deepfakes'), sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, misogynistic/misandrist messages and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- We recognise that harmful sexual behaviour (HSB) exists on a continuum, from behaviour that may be developmentally appropriate to behaviour that is abusive or violent, and that child-on-child abuse is a safeguarding issue for both the victim and the alleged perpetrator.
- We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We 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

between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSHE curriculum and through our active tutorial programme.

- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We 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.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputies) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our positive behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, 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 (or deputies) will discuss this with Sussex 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.

7.2 Making or Sharing Nudes and Semi-Nudes (including AI-generated images)

- We recognise the making or sharing of nudes and semi-nudes as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputies).
- In line with Keeping Children Safe in Education 2026, 'making or sharing nudes and semi-nudes' refers to the creation, sending or posting of nude or semi-nude images (including photographs, videos and livestreams) by young people under the age of 18. Images may be taken by the child themselves or taken or created by another person, and may be digitally altered or wholly generated using artificial intelligence, including what are sometimes described as 'deepfakes' or 'deep nudes'.
- All incidents involving the making or sharing of nudes or semi-nudes, whether consensual or non-consensual, will receive a safeguarding response.
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of making or sharing nudes and semi nudes by

implementing preventative approaches, via a range of age and ability appropriate educational methods.

- We will ensure that all members of the community are aware of sources of support regarding the making or sharing of nudes and semi-nudes.
- We will respond to concerns regarding the making or sharing of nudes and semi-nudes, regardless of whether the incident took place on/off site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being nudes or semi-nudes of children, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented. In most instances, the images should not be viewed.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. nudes or semi-nudes of children, including AI-generated images) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of nudes or semi-nudes, we will:
    - Act in accordance with our child protection policy.
    - Ensure the DSL (or deputies) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
    - Store the device securely.
        - If an 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.
    - Carry out a safeguarding risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Children's Social Care and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions 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 UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people 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.
    - 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.

7.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- We will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputies).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant East Sussex Safeguarding Child Partnership's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If learners at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

7.4 Indecent Images of Children (IIOC)

- We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We recognise that indecent images of children include images that have been digitally altered or wholly generated using artificial intelligence (AI); these will be responded to in the same way as any other indecent image of a child.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet service provider (ISP) which implements appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy DSL) is informed, who will investigate the incident.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy DSL) and headteacher are informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted once directed to by the police.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

7.5 Cyberbullying

- All staff will understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, including prejudice-based and discriminatory bullying, will not be tolerated here.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which can be requested from the main office.

7.6 Cybercrime

- We will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

7.7 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at our setting and will be responded to in line with existing policies, including anti-bullying and behaviour.
- We recognise that racism, faith-targeted abuse, misogyny/misandry and other forms of discriminatory behaviour online are safeguarding issues and may constitute child-on-child abuse. We will promote an inclusive, anti-discriminatory culture where these behaviours are recognised, challenged and addressed as part of our safeguarding responsibilities.
- 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 (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

7.8 Online Radicalisation and Extremism

- We will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. We have Securly filtering and Monitoring which screens and highlights any websites of concern.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

8. Safer Use of Technology

8.1 Classroom Use

- We use a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
    Other games-based technologies
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - Key Stage 2
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
  - Key Stage 3, 4, 5
    - Learners will be appropriately supervised when using technology, according to their ability and understanding.

8.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

8.3 Filtering and Monitoring

- The school is compliant with the DfE's filtering and monitoring standards for schools and colleges. This is checked and reviewed at least once every academic year using the checklist appended to this policy.

8.3.1 Decision Making

- Our governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking," as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances and is reviewed at least once every academic year.

The review is led by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT service provider and is reported to the governor responsible for safeguarding/online safety. It includes checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record of these checks is kept. A review will also be conducted following the identification of a safeguarding risk or any changes in working practice such as remote access or Bring Your Own Device or if new technology is introduced. We follow the guidance outlined in the DfE filtering and monitoring standards when conducting the review and use the DfE 'Plan technology for your school' service to self-assess against the standards.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate using the Safer Internet Centre guidance on appropriate filtering and appropriate monitoring.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.
-

8.3.2 Filtering

- Education broadband connectivity is provided through SchoolsICT systems.
- We use Securly, a Network Web Filter, using "content-aware filtering technology", which blocks sites which contain, including, but not limited to: pornography, racial hatred, extremism, gaming and sites of an illegal nature
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The system blocks all sites on the Counter Terrorism Internet Referral Unit (CTIRU) list.
- We work with SchoolsICTto ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites:
    - Teachers will turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.
- If a member of staff would like a site to be blocked/unblocked, they will complete a request form (Appendix 1) and submit it to the DSL who will decide on an outcome.
- M-Tech have been advised that they should only take filtering requests from the DSL.

8.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

  - The use of Senso Cloud monitoring technology, which allows the teacher to monitor students' screens in real-time. Teachers (and the DSL) are alerted to breaches, and are able to lock their screen, take control of their screen, turn off their internet access, close tabs, send them a message, or end their session immediately.
  - Physical monitoring (supervision) by members of staff
  - Senso Cloud reports sent weekly to the DSL.
  - Active/pro-active technology monitoring services via the Securly software and reporting.
- If a concern is identified via monitoring approaches:
  - Concerns will be added to MyConcern and the DSL or deputies will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

8.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with data protection laws (the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025).
  - Full information can be found in our information security policy.

8.5 Security and Management of Information Systems

- We adhere to and meet the DfE cybersecurity standards.
- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be requested through the office.

8.5.1 Passwords

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 6 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Use a separate password for your work and personal accounts.

- Change passwords regularly.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.
- Use two factor verification for all accounts which have access to personal or sensitive operational data and functions.
- Store passwords securely.

8.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

8.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

8.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform Tri Townshend if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

8.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents. Staff are not expected to respond to e-mails outside the hours of 8am-6pm on a school day or at weekends.

8.8.2 Learner email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

8.9 Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.
- When planning the use of live stream platforms within remote learning our school will:
    - Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
    - Ensure that staff are trained to use the technology.
    - Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
    - Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense. What follows next is more relevant, but not exclusively, to the use of platforms allowing two-way video interaction between all users.

- Two members of staff will be 'within the room' when conducting a live stream session with pupils. If the session is being run from school and both adults are there, then they can be physically within the same room. If one or both adults are working remotely then this means that two adults will need to be present within the video call, and they should both be there before the pupils dial in.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or recording features if these cannot be disabled.

- It is the responsibility of the staff member to act as a moderator, raising any issues of suitability (dress, setting, behaviour etc.) with the child and/or parent immediately and ending the online interaction if necessary.
- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.
- Staff will use school devices and school contact numbers/emails for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Pupils should be dressed appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
- Pupils should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay.

Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, the content will be monitored by a member of staff along with the interactions/behaviour of the learners taking part.
- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and, then, monitor some sessions to check they are in accordance with the policy.
- We are aware that our filtering and monitoring systems may not necessarily prevent inappropriate content from being shared in a live-streamed event as it is happening in real-time.

Using video calls for 1:1 sessions with children

- The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT and parental consent given.
- Where the communication with an individual child does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.

- In either case both adults will be present before the child is admitted to the online session.

8.10 Management of Learning Platforms

- We use Microsoft Teams, Seneca and various other platforms as our official learning platforms.
- Leaders and staff will regularly monitor the usage of the Learning Platforms (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

8.11 Management of Applications (apps) used to Record Children's Progress (If used)

- We use 'Engage' to track learners progress and share appropriate information with parents and carers.
- The Headteacher/manager is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection laws (the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025).
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8.12 Generative Artificial Intelligence (AI)

- We recognise that generative AI offers opportunities for teaching, learning and workload, but also brings safeguarding risks, including exposure to harmful or inaccurate content, AI applications that simulate interaction with other users (such as chatbots and 'companion' apps), AI-generated or digitally altered images including 'deepfakes', and risks to personal data.
- Our use of generative AI follows the DfE guidance Generative artificial intelligence in education and Generative AI: product safety expectations. Only generative AI tools that have been risk assessed and approved by the Senior Leadership Team will be used with, or by, learners.
- Staff will not enter personal or sensitive information about learners, families or colleagues into generative AI tools unless the tool has been approved for that purpose, in line with data protection laws and our GDPR Policy.
- Staff will be supported to use AI safely and effectively, including through the DfE's online AI resources for education staff, which cover identifying and mitigating risks associated with safeguarding, ethics, data protection and intellectual property.
- Our filtering and monitoring arrangements, and the annual review of their effectiveness, will take account of how generative AI tools are accessed on school devices and networks.
- Learners will be taught about the benefits and risks of AI, including deepfakes, AI-generated misinformation and the risks of relying on AI chatbots for advice or friendship, through our computing, PSHE/RSHE and active tutorial programmes.
- Any concern involving generative AI, including the creation or sharing of AI-generated nudes or semi-nudes, indecent images, or content used to bully or harass, will be reported to the DSL (or deputies) and responded to in line with section 7 of this policy and our child protection policy.

9. Social Media

9.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of our community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of our community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of our community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site. Social Media sites are blocked on the filtering and monitoring system.
    - The use of social media during setting hours for personal use is not permitted.

    - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of our community on social media, should be reported to the DSL (or deputies) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct/ Staff behaviour policy as part of Acceptable Use Policy.

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 setting.
    - 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 sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of our setting on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners 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.

Communicating with learners and parents and carers

- Communication with children both in the offline world and through web based and telecommunication interactions should take place within explicit professional boundaries. This

includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

- Staff should not give out any personal contact details.
- On school trips, staff should have a school mobile phone rather than having to rely on their own device.
- Staff should not accept friend requests from pupils, past or present. If a member of staff feels that this is necessary, they should first seek guidance from the DSL or a senior leader. If ongoing contact with learners 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. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher (see Staff Behaviour Policy/ Code of Conduct for further information)
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher/manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).
-

9.3 Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details 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 by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only 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 both within the setting and externally.

- To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.
- How AI-generated images and 'deepfakes' can be created and misused, and what to do if they are worried about an image of themselves or others.

9.4 Official Use of Social Media

- Our official social media channels are on:
  - Facebook page
  - YouTube channel
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
  - 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 channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage any official social media channels.
  - Official social media sites are suitably protected and, where possible, run and linked to our website.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including anti-bullying, image/camera use, data protection, confidentiality and child protection.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated possible.
- Parents and carers will be informed of any official social media use with learners; 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.

Staff expectations

- 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 participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our social media acceptable use policy.

- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.
- Always be 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.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- 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 direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

10. Use of Personal Devices and Mobile Phones

- We recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

10.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Positive Behaviour, Child Protection and Staff Code of Conduct.
- 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 mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in school. In line with the DfE statutory guidance Mobile phones in schools and Keeping Children Safe in Education 2026, Northease Manor School is a mobile phone-free environment for learners by default; any exception is by agreement with the Headteacher only.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

10.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place e.g. locked in a drawer) during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the headteacher/manager, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and Headteacher
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons or educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

10.3 Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- In line with the DfE statutory guidance Mobile phones in schools, learners do not have access to their mobile phones throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime.
- We expect learners' personal devices and mobile phones to be…
    - Handed in to their tutor or kept in a secure place if they are in Lower School or Middle School, or, if they are in Senior School or Sixth Form, never used, seen, or heard between the hours of 08:30 and 16:00.
- If a learner needs to contact their parents or carers they will be allowed to use a setting phone e.g. the office phone or in pastoral
- Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher

- Mobile phones or personal devices will not be used by learners during lessons or formal educational time
- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
- Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, they will receive reminders on the first two occasions that this happens. On the third occasion, the DSL will write to the learner's family, instructing them to keep the device at home for a period of one week.
- Consistent breaches of the policy may see the development of Safeguarding Risk Reductions Plans, or Risk assessments being drawn up.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our Positive behaviour or anti bullying policy or could contain nudes or semi-nudes (including AI-generated images). However, staff are not to look at any images that may be illegal.
- Searches of mobile phone or personal devices will only be carried out in accordance with www.gov.uk/government/publications/searching-screening-and-confiscation)
- Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies www.gov.uk/government/publications/searching-screening-and-confiscation)
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

10.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headteacher of any breaches our policy.

10.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required of site.
- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

11.Useful Links for Educational Settings

East Sussex Support and Guidance:

- East Sussex County Council Early Years Support & Intervention Team
  - Call: 01323 463026
  - Email: childcare.support@eastsussex.gov.uk
- If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on 01323 464222 or 0-19.SPOA@eastsussex.gov.uk
- Standards and Learning Effectiveness Service (SLES): SLES.Safeguarding@eastsussex.gov.uk

East Sussex Support and Guidance for Educational Settings

- https://czone.eastsussex.gov.uk/safeguarding/

East Sussex Safeguarding Children Partnership

- www.sussexchildprotection.procedures.org.uk/

Sussex Police:

- www.sussex.police.uk

For non-urgent Police contact 101

If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: Net-Aware
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Get Safe Online: www.getsafeonline.org
- Action Fraud: www.actionfraud.police.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)

- DfE Keeping children safe in education 2026: www.gov.uk/government/publications/keeping-children-safe-in-education--2
- DfE Generative artificial intelligence (AI) in education: www.gov.uk/government/publications/generative-artificial-intelligence-in-education
- DfE Mobile phones in schools (statutory guidance): GOV.UK
- DfE Plan technology for your school (filtering and monitoring self-assessment): GOV.UK

National Links and Resources for Professionals/Parents/Carers

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2026 Part 2 for more resources.

Formatted: Not Highlight

Formatted: Underline, Font colour: Custom Colour (RGB(5,99,193))

Appendix 1: Request to Filter a Website Form

	A	B	C	D	E
1	**Request to Filter Website**				
2					
3	**Name of Requester**	**Date**	**Site URL (eg. www.bbc.co.uk/sport)**	**Rationale**	
4					
5					
6					
7					
8					
9					
10	**FOR DSL ONLY**				
11					
12	**Block Site Yes/No**	**Date**	**M-Tech Ticket Number**		
13					
14					
15					
16					
17					
18					