ONLINE SAFETY POLICY

Autumn 2021

This policy will be reviewed <u>at least</u> annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

Key Details

Designated Safeguarding Leads:

Anne Siggins (Executive Headteacher)
Kelly Brown (Headteacher Priory Fields School)
Helen Thompson (Headteacher St Martin's School)
Lisa Sprigmore (Headteacher Vale View School)

Named Governor with lead responsibility

Malcom Bowler – Priory Fields School
Mike Ashley - Vale View and St Martin's School

Named Trustee with lead responsibility

Patricia Sherling

Online Safety Vision

Pupils to become confident, competent, independent and safe users of ICT in this rapidly developing technological world.

1. Policy aims

This online safety policy has been written by Ruth Bishop involving staff and pupils building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.

The purpose of this online safety policy is to:

- Safeguard and protect all members of the school 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.

Whinless Down Academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

WDAT believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online. It identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. WDAT believes that pupils 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 school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct
- Behaviour and discipline policy
- Child protection and safeguarding policy

- Confidentiality policy
- GDPR policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data security
- Image use policy
- Mobile phone and social media policies
- Searching, screening and confiscation policy

Monitoring and Review

- Technology in this area evolves rapidly. WDAT will review this policy at least annually. The policy will also be revised following any national or local policy requirement and any child protection concerns or any changes to the technical infrastructure
- We will ensure that we 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 Head of School/DSL will be informed of online safety concerns, as appropriate.
- Safeguarding will be reported to the governors on a regular basis, and then ultimately to the trustees of the academy.
- Any issues identified will be incorporated into the school's action planning.
- The WDAT has appointed a Designated Safeguarding Lead at each school to be the online safety lead.

2. Key responsibilities

The Designated Safeguarding Lead has lead responsibility for online safety. WDAT recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The key responsibilities of the school management team are:

- Ensure that online safety vision is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety, including an AUP.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of schools systems and networks.

The key responsibilities of the DSL are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends and communicate with the school community as appropriate.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Maintaining logs on Cura of any online safety incidents and the actions taken; as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the policies and procedures.
- Ensure all members of staff receive regular up-to-date and appropriate online safety training.
- Work with staff to co-ordinate participation in local and national events to promote positive online behaviour such as Safer Internet Day.
- Report online safety concerns on Cura, as appropriate, to the leadership team.
- Review any online safety policies, including AUPs and other policies and procedures.

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policy (AUPs) and adhering to them.
- Comply with all GDPR regulations and policies
- Take responsibility for the security of school systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls / encryption are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the DSL.
- Report any breaches or concerns to the designated safeguarding lead and leadership team and together ensure that they are recorded on Cura, and appropriate action is taken as advised.
- Providing technical support and perspective to the leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies/online rules and adhering to them.
- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Engage in age appropriate online safety education opportunities.

The key responsibilities of parents and carers are:

- Reading the schoo Acceptable Use Policy, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Support the school by discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Abide by the schools home-school agreement.

3. Education and Engagement Approaches

Education and engagement with learners

- The school has a progressive online safety curriculum which raises awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in PSHE and computing teaching.
    - 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.

- The school will support learners to read and understand the acceptable use policy in a way which suits their age and ability by:
    - Displaying 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.
    - 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.

Vulnerable Learners

WDAT recognises that some 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. The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. When implementing an appropriate online safety policy and curriculum the school will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

Training and engagement with staff

WDAT 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 on a regular basis, with at least annual updates. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- 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.
- 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.

Awareness and engagement with parents and carers

- WDAT recognises 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.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - 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.

Reducing Online Risks

- WDAT recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- 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 to members of the community. This is clearly outlined in our acceptable use policy and highlighted through a variety of education and training approaches.

4. Safe Use of Technology

Classroom Use

- WDAT uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Intranet
    - Email
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policy 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.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners 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 learners age and ability.

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.

Filtering

- WDAT governors and leaders have ensured that the schools have 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.
- 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.
- 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.
- Education broadband connectivity is provided through Eis/Cantium.
- We use Eis/Cantium filtering which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Eis/Cantium to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - 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 and/or Headteacher.
    - 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, Kent Police or CEOP.

Monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by: physical supervision, and monitoring internet and web access.
- If a concern is identified via monitoring approaches the DSL or deputy 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.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and Management of Information Systems

- 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 or access via appropriate secure remote access systems.
    - 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 but the youngest users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- 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 1 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.
    - Change their 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.

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 administrators account for our website will be liked to school email accounts and secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

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: image use, data security, GDPR, acceptable use policies, codes of conduct/behaviour, social media and use of mobile technology.
- Staff must ensure they follow the academy procedure for the publication of any photos of children.

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.
    - 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 tell the DSL/Headteacher if they receive offensive communication, and this will be recorded in our safeguarding records (Cura).
- 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.

Staff email

- The use of personal email addresses by staff, governors or trustees 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.

Learner email

- Learners may 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.

Educational use of Videoconferencing and/or Webcams

WDAT recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.

- Microsoft Teams is used for remote learning. It is the responsibility of the parents to ensure safe use for the child. Staff to report any safeguarding concerns via the normal channels.

- All videoconferencing and webcam equipment used in school will be switched off when not in use and will not be set to auto-answer. Staff will ensure that videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure. Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

- Iris video conferencing tool is used to support monitoring and staff CPD. Recordings are owner by the individual recording.

Users

- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment e.g. Microsoft Teams.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and will be stored securely within Teams.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

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

- The Headteacher 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 legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - 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.

5. Responding to Online Safety Incidents and Concerns

- All members of the community are aware of the reporting procedure for online safety concerns, including: breaches of filtering, sexting, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- 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.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police.
- 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 will speak with Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

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

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher in accordance with the allegations policy.

- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- WDAT recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, 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.
- WDAT recognises that 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.
- WDAT also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- WDAT 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 curriculum.
- 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 deputy) 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 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 Services 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 deputy) will discuss this with Kent 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.

Youth Produced Sexual Imagery ("Sexting")

- WDAT recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- WDAT will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' 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 youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
  - We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
  - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding 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 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 Services and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- 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 UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding 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.

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

- WDAT 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.
- WDAT recognises 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 deputy).
- 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 on the schools home page (website).
- 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 Kent Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police

    - Carry out a risk assessment which considers any vulnerabilities of learner(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 Education Safeguarding Team and/or Kent Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- WDAT will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 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 subscribes to the Internet Watch Foundation 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 (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent 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) is 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.
    - 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) is 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.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (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 Head of School 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.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at WDAT.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at the school and will be responded to in line with existing policies, including 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 (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

Online Radicalisation and Extremism

- 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.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) 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 Head of School will be informed immediately, and action will be taken in line with the child protection and allegations policies.