WHITE ROSE ACADEMIES

Online Safety Policy

Author / Lead	Director of Safeguarding
Approval date	*Pending Approval at Oct 25 Board Meeting*
Review interval (years)	Annual
Review date	September 2026
Target audience	All staff, Governors, Trustees

Leeds City Academy Leeds East Academy Leeds West Academy ALDER TREE PRIMARY BELIEVE - BELONG - BECOME

Contents

1. Introduction and Purpose

White Rose Academies Trust (WRAT) is committed to promote the welfare and safety of our students in all of our academies when using digital and online technologies. WRAT recognises the importance of the contribution it can make to protecting and supporting students across its academies in their use of these technologies.

This policy is designed to incorporate all aspects of child protection and safeguarding that may be affected by digital technology, mobile phone technology, as well as WRAT's use of technology within its academies.

The organisation will refer to the most recent government, Department for Education (DfE) and Information Commissioners Office (ICO) guidance and documentation with regard to data protection, data storage and privacy compliance.

2. Scope

This policy applies to all WRAT staff (including agency), pupils/students, parents/carers, trustees, governors, contractors, ambassadors and other volunteers.

This policy applies to any individual who is given access to WRAT's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the organisation).

The WRAT expects all academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour - as defined as regulation or student behaviour under the Education and Inspections Act 2006. The 'In Loco Parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material, including reporting to the police, social media websites, and hosting providers on behalf of students.

3. Aims

All academies within the WRAT aim to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, misinformation, racism, misogyny, self-harm, suicide, antisemitism, radicalization and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gaming, gambling, inappropriate advertising, phishing and/or financial scams.

4. Legislation and Guidance

This policy is underpinned by the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE), September 2025, which outlines schools' responsibilities to protect pupils from all forms of harm, including online abuse, exploitation, and radicalisation. The guidance emphasises the importance of robust filtering and monitoring systems and the need for a whole-school approach to online safety.

It also draws on a range of current DfE guidance and statutory documents, including:

- Teaching online safety in schools
- Preventing and tackling bullying, including Cyberbullying: Advice for Headteachers and School Staff
- Relationships, Sex and Health Education (RSHE): Statutory Guidance (updated for September 2025), which includes strengthened requirements relating to online relationships, pornography, digital consent, and age-appropriate teaching of online harms
- Searching, Screening and Confiscation: Advice for Schools (2024)
- Meeting Digital and Technology Standards in Schools and Colleges, including the Filtering and Monitoring Standards (2024)
- Education for a Connected World framework
- Guidance on protecting children from radicalisation, including the Prevent Duty under the Counter-Terrorism and Security Act 2015

This policy reflects key legislation, including but not limited to:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Education Act 2011 (empowering staff to search for and delete inappropriate digital material for safeguarding purposes)
- Equality Act 2010
- Data Protection Act 2018 and UK GDPR
- Online Safety Act 2023, which introduces new statutory duties for online service providers and reinforces schools' roles in educating pupils about digital safety, content regulation, and harmful online behaviours

It also aligns with the National Curriculum computing programmes of study, which promote digital literacy, responsible use of technology, and understanding of online risks.

This policy complies with the school's funding agreement and articles of association, and forms part of our wider safeguarding and child protection framework.

5. Roles and Responsibilities

All roles and responsibilities outlined in this section reflect the Trust's compliance with the latest statutory guidance and legislation, including:
Keeping Children Safe in Education (KCSIE) 2025, the Online Safety Act 2023, the DfE Filtering and Monitoring Standards (2023), and the updated RSHE Guidance (2025). It also aligns with the requirements of the Data Protection Act 2018, UK GDPR, and relevant guidance such as *Data Protection in Schools (2023)* and UKCIS best practices.

5.1 Trustees

The delegated trustee for safeguarding will liaise with the Trust Director of Safeguarding and each Local Accountability Board (LAB) to:

- Monitor the effectiveness of online safety strategy across all academies.
- Review incidents, filtering and monitoring data, and compliance with statutory obligations such as those outlined in the Online Safety Act 2023 and the DfE's filtering and monitoring standards.
- Ensure governance reflects the strategic importance of online safety within broader safeguarding frameworks.

5.2 Executive Team

The Executive Principal, through line management, will:

- Ensure the Trust and its academies are implementing a whole-school approach to safeguarding, as defined in *KCSIE 2025*, which includes embedding online safety across curriculum, policy, and practice.

- Support and challenge the Director of Safeguarding and the Director of IT, who will:
  - Lead the annual review of the online safety policy in line with emerging legislation, technologies, and incidents.
  - Audit filtering and monitoring systems to meet or exceed DfE standards.
  - Support academies to complete the Trust-wide Prevent and Online Safety Audit, which informs strategic planning.

5.3 Local Accountability Board (LAB)

Each LAB holds responsibility for local oversight of online safety and will:

- Review and approve the policy, ensuring it aligns with statutory duties and includes provisions outlined in the Online Safety Act 2023 and RSHE Guidance 2025.
- Use the UKCIS resource "*Online safety in schools and colleges: Questions from the Governing Board*" to monitor and evaluate policy effectiveness.
- Appoint a link safeguarding governor responsible for overseeing online safety compliance, referencing DfE standards and guidance at safefiltering.lgfl.net.
- Ensure online safety is integrated into the curriculum and adapted for vulnerable children, including those with SEND or a history of trauma.
- Oversee compliance to mandatory safeguarding training for all staff and governors, with a focus on online harms, filtering/monitoring, and contextual safeguarding.
- Work with DPOs and DSLs to balance child protection and data protection, ensuring lawful, safe information sharing.

5.4 Academy Principal

The Principal is responsible for:

- Ensuring that all staff consistently apply this policy.
- Embedding online safety within the curriculum and wider safeguarding framework, per *KCSIE 2025* and *RSHE Guidance 2025*.
- Ensuring that online safety measures (technical and educational) align with national standards and statutory expectations.

5.5 Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for managing online safety and will:

- Support the Principal in implementing policy and addressing incidents.
- Liaise with IT staff and external providers (e.g., Smoothwall) to manage technical safety concerns.
- Ensure logs of online safety and cyberbullying incidents are accurate and reviewed.
- Coordinate with external agencies as needed (e.g., police, LADO, Prevent).

- Ensure staff receive ongoing training and updates on the latest risks and legislative changes, including new guidance from *KCSIE 2025*, *the Online Safety Act*, and *RSHE*.
- Report to the LAB and the Director of Safeguarding on patterns, gaps, and incidents.

5.6 Director of IT

The Director of IT is responsible for ensuring cyber and data security across Trust systems by:

- Implementing filtering and monitoring systems in compliance with DfE Filtering and Monitoring Standards and the Online Safety Act 2023.
- Ensuring firewalls, antivirus, and malware protections are up to date and reviewed regularly.
- Conducting security checks and access audits each half term.
- Blocking harmful content and working with DSLs to investigate breaches.
- Supporting strategic decision-making around the safeguarding implications of digital tools and platforms.
- Ensuring staff understand how filtering and monitoring contributes to safeguarding.

5.7 All Staff and Volunteers

All staff (including agency staff and volunteers) must:

- Adhere to the acceptable use policy (Appendix 4) and ensure pupils do the same.
- Undertake regular safeguarding training, including updates specific to online safety, filtering and monitoring, sexual harassment online, and youth-produced imagery.
- Report all incidents using the Trust's systems (e.g., CPOMS), whether online or offline in nature.
- Maintain awareness of the wide range of online harms (outlined in *KCSIE 2025*) and apply a contextual approach when dealing with disclosures or concerns.

5.8 Data Protection Officer (DPO)

The DPO ensures data protection compliance while prioritising safeguarding, and will:

- Deliver GDPR and data security training and guidance for staff.
- Ensure compatibility across data policies, online safety, and safeguarding measures.
- Monitor and limit access to safeguarding data and ensure retention policies are followed.
- Reinforce DfE guidance that data protection laws do not prevent the lawful sharing of safeguarding information, as outlined in *KCSIE 2025* and *Data Protection in Schools (2023)*.

5.9 Parents

Parents are expected to:

- Read and support the Acceptable Use Policies (Appendices 1–3).
- Report concerns related to online safety.
- Access guidance from recognised organisations such as:
  - UK Safer Internet Centre
  - Childnet International
  - National Crime Agency CEOP Education

5.10 Visitors and Community Users

All visitors who access academy IT systems or networks must:

- Be made aware of this policy.
- Agree to and follow the Acceptable Use Policy (Appendix 4), where applicable.

6. Educating Students About Online Safety

Students will be explicitly taught about online safety as part of a whole-school approach to safeguarding, embedded across the computing curriculum, RSHE, and relevant subject areas in accordance with KCSIE 2025 and the RSHE Guidance 2025.

Teaching will reflect age-appropriate content from the Education for a Connected World Framework, and will include critical areas such as online relationships, digital resilience, consent, pornography, cyberbullying, misinformation, online abuse, and the impact of technology on mental health.

Key Stage 1 (Ages 5–7)

Pupils will learn to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support if they are worried about anything seen or experienced online.
- Understand that not everything they see online is true.

Key Stage 2 (Ages 7–11)

Pupils will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable online behaviour.
- Identify and report concerns about content, contact, and conduct online.
- Understand how to critically assess what they see online and question reliability.

- Recognise that people may behave differently online, including pretending to be someone they are not.
- Know the principles of respectful online communication, even when anonymous.
- Understand risks associated with sharing personal information or communicating with strangers.
- Know that their online actions have real-world consequences and legal implications.

By the end of primary school, students will also understand:

- How to stay safe online, including the importance of strong passwords and reporting harmful content.
- The implications of digital footprints and data sharing online.
- What safe and appropriate boundaries look like, including in online friendships.
- That online content can be manipulated or fake (e.g. deepfakes or misinformation).

Key Stage 3 (Ages 11–14)

Students will be taught to:

- Use technology safely, securely, and responsibly, including protecting their digital identity and privacy.
- Recognise different types of harmful online behaviours such as grooming, exploitation, harassment, coercive control, or exposure to extremism.
- Understand the psychological and emotional impact of online harms and how to seek help.
- Identify, avoid, and report online scams, hoaxes, and phishing.
- Understand the legal and social implications of online activity, including youth-produced sexual imagery (sexting).

Key Stage 4 (Ages 14–16)

Students will learn to:

- Understand the rapid development of technology and its impact on online safety and digital wellbeing.
- Recognise how material can be shared beyond its intended audience and the challenges in removing content.
- Know how to seek support if affected by online abuse or exploitation, including through CEOP or other external agencies.
- Understand that viewing or sharing indecent images of children (even if self-generated) is illegal and can result in serious criminal consequences.

- Analyse and reflect on how pornography distorts attitudes to sex and relationships, impacts mental health, and perpetuates harmful stereotypes (per RSHE Guidance 2025).
- Navigate the risks associated with social media platforms, influencers, algorithms, and echo chambers.
- Understand digital consent: how it applies to image sharing, communication, and sexual relationships, and how consent can be given or withdrawn.

By the end of secondary education, all students will know:

- That their rights, responsibilities, and expectations for respectful behaviour apply equally online and offline.
- How to respond to and report different types of online concerns, including sexual harassment, hate speech, bullying, abuse, radicalisation, and scams.
- The influence of online content and platforms on body image, self-esteem, and peer pressure.
- How to use social media safely and manage privacy settings.
- How online information and data is generated, collected, used, and sold, including awareness of algorithmic targeting and the influence of AI.

Inclusion and Adaptation

In line with KCSIE 2025, teaching about online safety will be:

- Adapted to reflect the needs of vulnerable children, including pupils with SEND, those with social care involvement, victims of abuse, and children with limited access to technology.
- Delivered using a contextualised and trauma-informed approach where necessary.
- Supported through targeted small-group or one-to-one teaching where a differentiated approach is most effective.

Cross-Curricular Integration

- Online safety will be reinforced across computing, RSHE, citizenship, and safeguarding-themed assemblies or enrichment days.
- Current topics (e.g. AI, misinformation, digital wellbeing) will be woven into lessons to reflect emerging risks and real-life digital scenarios.
- External speakers or resources may be used to enhance delivery, provided they align with DfE and KCSIE vetting standards.

7. Educating parents about online safety

In line with Keeping Children Safe in Education (KCSIE) 2025, the RSHE Statutory Guidance 2025, the Online Safety Act 2023, and the DfE Filtering and Monitoring

Standards, the academy recognises that engaging and informing parents and carers is a critical part of our whole-school approach to online safety.

The academy will raise awareness of internet safety, digital wellbeing, and online harms through the following:

- Regular communications to parents and carers (e.g. newsletters, letters, and text/email alerts)
- Online safety resources and guidance published on the academy website
- Direct engagement at parents' evenings, curriculum briefings, or safeguarding workshops
- Sharing key updates from national guidance, including expectations from RSHE and online safety policy updates

The online safety policy will be made available to all parents and carers, both via the website and upon request. Parents will be informed of the scope of online safety education, including:

- The platforms, apps, and websites students are expected to use
- The filtering and monitoring systems used in school to protect students, in line with DfE standards
- Who students are interacting with online (e.g. staff, peers), and whether interactions are one-to-one or group-based
- How to access support or raise concerns about their child's online experiences

In line with the RSHE Guidance 2025, parents will be made aware that students are taught about a range of sensitive but essential age appropriate topics relating to online safety and relationships, including:

- The impact of pornography, including how it distorts expectations around sex, bodies, and relationships
- Understanding digital consent, and how consent can be communicated or withdrawn in online contexts
- Recognising coercion, exploitation, grooming, and image-based abuse, including the criminal consequences of sharing explicit material
- The effects of online harassment, misogyny, extremism, and harmful ideologies encountered on social platforms
- Building resilience to misinformation, including recognising manipulated content such as deepfakes

We will work in partnership with parents to ensure these messages are understood and reinforced at home. Where appropriate, parents will be provided with guidance to support sensitive conversations, and opportunities to raise concerns or ask questions about RSHE and online safety content.

Parents are strongly encouraged to take an active role in supporting their child's online learning and digital wellbeing, and to familiarise themselves with the risks young people face online.

Raising Concerns

Any concerns or queries regarding this policy they should be directed in the first instance to the Academy Principal.

Concerns about students' safety online or wider online safety provision can be raised with any staff member, who will ensure these are escalated appropriately.

8. Cyber-Bullying

8.1 Definition

In accordance with *Keeping Children Safe in Education (KCSIE) 2025* and the DfE's *Preventing and Tackling Bullying* guidance, cyber-bullying is defined as bullying that takes place online via social networking platforms, messaging apps, email, gaming sites, or any digital space. Like other forms of bullying, it involves:

- Intentional and repetitive harm
- A real or perceived power imbalance
- Behaviour that causes emotional, psychological, reputational, or physical harm

Cyber-bullying can take many forms, including but not limited to:

- Harassment or intimidation via messages, posts, or calls
- Exclusion from online groups
- Sharing embarrassing images or videos without consent
- Impersonation or fake profiles
- Threatening or coercive messaging
- Spreading rumours or misinformation

(See also the academy's Positive Relationships / Behaviour Policy.)

8.2 Preventing and Addressing Cyber-Bullying

In line with KCSIE 2025, the RSHE Guidance 2025, and the Online Safety Act 2023, the academy takes a proactive, educational, and preventative approach to tackling cyber-bullying.

We will:

- Teach students what cyber-bullying is, how it manifests, how it differs from in-person bullying, and what to do if they experience or witness it.
- Ensure students are aware of how to report online abuse or harmful behaviour, including confidential or anonymous channels where appropriate.

- Encourage students to report concerns even if they are bystanders, not direct victims.
- Embed cyber-bullying education across the curriculum, including in RSHE, computing, and PSHE, addressing digital respect, peer pressure, and online accountability.
- Ensure that teaching content reflects the age-appropriate risks outlined in *Education for a Connected World*, including harmful online challenges, image-based abuse, and the psychological impact of persistent online targeting.
- Ensure students understand the legal consequences of some online behaviours (e.g. malicious communications, harassment, revenge porn, or sharing indecent images of children).

Staff and Parental Engagement

- All staff and relevant volunteers receive training on cyber-bullying, its signs, impact, and safeguarding response as part of annual safeguarding and online safety training, updated regularly in accordance with new risks and legislation.
- Through their website the academy provides parents and carers with guidance on recognising signs of cyber-bullying, how to talk to their children about online harm, and how to respond to incidents (including reporting routes and external support).

Responding to Incidents

When responding to incidents of cyber-bullying:

- The school will follow procedures outlined in the academy Positive Relationships/ Behaviour Policy, Safeguarding and Child Protection Policy, and Online Safety Policy.
- The DSL will lead or support the investigation, in collaboration with the Principal and, where appropriate, the Director of Safeguarding or Director of IT.
- All incidents will be logged, and any digital evidence will be retained in line with data protection and safeguarding protocols.

Where material is deemed:

- Illegal (e.g. child sexual abuse imagery, threats of violence), the DSL will ensure it is reported to the police and appropriate authorities without delay.
- Harmful or inappropriate, the school will use reasonable and proportionate efforts to contain the incident, such as:
  - Supporting affected students
  - Requesting removal of content from platforms
  - Liaising with parents/carers
  - Working with online providers or law enforcement, if necessary

The DSL will not view or forward illegal content but will follow *UKCIS guidance on managing youth-produced sexual imagery*, and *DfE guidance on searching, screening, and confiscation (2024)* to determine appropriate next steps.

Supporting Victims

The academy is committed to ensuring that students who experience or witness cyber-bullying receive timely, compassionate, and appropriate support. This may include:

- Referral to internal pastoral support/counselling
- Enhanced monitoring or safety planning
- Regular follow-up with the student and their family
- Support in rebuilding peer relationships
- Referral to external services (e.g. mental health, police, CEOP), where required

Where needed, responses will be tailored to the needs of vulnerable students, including those with SEND or a history of trauma, in accordance with *KCSIE 2025*.

9. Examining Electronic Devices

In line with the Education and Inspections Act 2006 (as amended by the Education Act 2011), DfE guidance (2024), and KCSIE 2025, authorised academy staff have the statutory power to search a student's electronic device (such as a mobile phone, tablet, or laptop), where they have reasonable grounds to suspect that the device contains:

- Material that has been, or could be, used to cause harm
- Content that may disrupt teaching
- Evidence of a breach of academy rules (including the recording of other students or adults on site)
- Material that may constitute a criminal offence, including prohibited or harmful online content

9.1 Search, Screening and Confiscation

Any such search or screening will be conducted:

- Lawfully and proportionately
- By two staff members, one of whom must be the same sex as the student (except in exceptional circumstances)
- In accordance with the DfE's Searching, Screening and Confiscation guidance (2024) and with regard to student dignity and wellbeing

Where inappropriate or harmful material is found, a decision will be made by the authorised staff member in **consultation with the Designated Safeguarding Lead (DSL)** or a member of the **Senior Leadership Team (SLT)** as to whether the material should be:

- Deleted from the device (if lawful and proportionate to do so)
- Retained as evidence of a breach of academy discipline or a possible criminal offence
- Reported to the police, if there is reasonable belief the material is illegal

If staff have reasonable grounds to suspect that the device contains evidence of an offence, it will be confiscated and handed to the police without being viewed by school staff (unless advised to do so by the police).

9.2 Nude or Semi-Nude Images and Videos (Youth-Produced Sexual Imagery)

Where there is any suspicion that a device contains nude or semi-nude images or videos of a child (commonly referred to as "sexting"), the following steps will apply:

- Staff must not view, copy, or forward the content under any circumstances.
- The concern must be reported immediately to the DSL, who will make a risk-informed decision based on:
  - UKCIS guidance: *Sharing nudes and semi-nudes – advice for education settings*
  - *KCSIE 2025* and *DfE Searching, Screening and Confiscation (2024)*
  - Whether the incident involves coercion, exploitation, grooming, or criminality
- If the imagery is believed to be illegal, the DSL will inform the police and follow the appropriate safeguarding procedures.
- The DSL may consult with children's social care or external safeguarding professionals, where appropriate.

9.3 Data Protection and Record Keeping

- Any action taken regarding confiscated devices or deleted material must comply with the Data Protection Act 2018 and UK GDPR.
- A clear record must be kept of:
  - The reason for the search
  - Who conducted the search
  - What was found and any actions taken (deletion, referral, retention)
  - Whether the incident was escalated to the police or safeguarding authorities

All records will be stored securely in line with the academy's data protection and safeguarding policies.

9.4 Complaints

Any concerns or complaints regarding the search or examination of a student's electronic device will be managed in accordance with the **academy complaints**

procedure. Parents/carers have the right to request further information and raise concerns if they believe the process has not been conducted appropriately or lawfully.

10. Acceptable Use of the Internet in School

The academy promotes a safe, responsible, and respectful approach to internet use, in line with KCSIE 2025 and the Online Safety Act 2023.

All students, parents, staff, volunteers, trustees, and governors are required to sign and adhere to an Acceptable Use Agreement (AUA) relevant to their role (see Appendices 1 to 4). Visitors may also be asked to read and agree to the academy's acceptable use expectations where access to ICT systems is granted.

Use of the academy's internet and digital devices is for:

- Educational purposes only (for students)
- Work-related use only (for staff, governors, and volunteers)

To uphold compliance with the DfE's filtering and monitoring standards, the academy uses appropriate systems to:

- Filter inappropriate content
- Monitor digital activity on the network
- Detect signs of harm, abuse, or misuse, in accordance with our safeguarding protocols

Monitoring is conducted in line with the school's privacy, safeguarding, and data protection policies. Breaches of acceptable use will be addressed in accordance with relevant disciplinary procedures.

11. Students Using Mobile Devices in School

In accordance with KCSIE 2025, RSHE 2025, and the school's behaviour and safeguarding policies:

- Students may bring mobile phones and other personal devices onto the school site at their own risk, but these must be switched off and kept out of sight during the school day, unless specific permission is granted by a member of staff.
- The use of mobile devices is only permitted when explicitly authorised for a defined educational purpose under staff supervision.
- Smartwatches with messaging, camera, or recording capability are also subject to these same restrictions.
- Any use of a mobile or personal device must comply with the student's Acceptable Use Agreement (see Appendices 1–3).

Breaches of this agreement may lead to:

- Confiscation of the device in line with DfE guidance on searching, screening and confiscation (2024)

- Parental notification
- Disciplinary action, in accordance with the academy behaviour policy

The academy and the WRAT do not accept liability for the loss, damage, or theft of personal mobile devices brought onto school premises.

12. Staff Using Work Devices Outside the Academy

All staff must use work devices responsibly and securely, in accordance with:

- The academy's Acceptable Use Agreement (Appendix 4)
- KCSIE 2025
- The Data Protection Act 2018 / UK GDPR
- Internal safeguarding, IT, and data handling protocols

To maintain security, staff must ensure that work devices:

- Are password-protected using strong credentials (minimum 8 characters including uppercase, lowercase, numbers, and symbols)
- Have encryption enabled to prevent unauthorised access if lost or stolen
- Automatically lock after a short period of inactivity
- Are not shared with family or friends
- Are regularly updated, including antivirus and software patches
- Are not used for personal browsing, file storage, or non-educational purposes

Staff are also reminded that:

- Any loss or compromise of a device or suspected data breach must be reported to the Designated Safeguarding Lead (DSL) or senior leadership immediately
- Devices must only be used to access and handle data in line with the staff member's professional role and safeguarding responsibilities

11. Social Media Contact with Students

Staff must not seek or establish contact with students via social media or other personal digital platforms for the purpose of forming or strengthening relationships. This applies even if the student initiates contact. Any such contact must be reported immediately to the Principal or line manager.

To maintain safer working practices and professional boundaries, all communication with students must occur through approved school channels, during school hours, using school equipment, and with appropriate permissions from senior leadership.

Staff must not share personal contact details (e.g., mobile numbers, personal email addresses, or social media handles) with students. Unauthorised contact may result in disciplinary action.

Internal email and approved communication platforms must be used in accordance with school policies and will be monitored for safeguarding purposes.

12. Mobile Technologies and Removable Media Devices

Mobile and removable media devices (e.g., laptops, tablets, USBs) are vulnerable to viruses, loss or theft. The Trust IT team has taken steps to limit their use across the network.

Exceptions to this control may be updated by IT if authorised by a senior staff member. Only essential and authorised data should be stored or transferred. Deleted data may still be recoverable, so secure deletion practices must be followed.

Staff must take all reasonable precautions to prevent data breaches, including physical protection and encryption where applicable.

Removable media must not be used for long-term storage or archiving of school records. Devices not issued by the Trust must not be used for official business or connected to Trust-owned equipment without written approval.

In line with KCSIE 2025 and the Data Protection Act 2018, staff may be held accountable if personal data is lost or stolen due to negligence.

13. Use of Digital and Video Images

Staff will educate students about the risks of creating, sharing, and publishing digital images, especially on social media and risks related to privacy, consent, and online exploitation.

Images of students may be taken only with written parental consent and must be captured using school-issued equipment. Personal devices must not be used, including during off-site activities, unless explicitly authorised by the Principal and transferred immediately to the Trust's secure network.

Images must be carefully selected to ensure that students are appropriately dressed and engaged in activities that reflect the values and standards of the school. Under no circumstances should students record, capture, or share images or videos of others without explicit consent, whether on school premises or during offsite school activities.

All schools within the Trust should apply the following best practice principles when using images of children:

- "Names-No-Images / Images-No-Names" unless there is specific consent for both to be used simultaneously.
- Metadata (e.g., location data) must be removed before uploading images.

- Images should be stored securely and shared only via approved platforms.
- Staff must receive regular training on image use and data protection.

Parents and carers are welcome to take photographs or videos of their own children during school events for personal use. However, they must refrain from sharing images or recordings that include other students or staff on public platforms or social media, to respect privacy and safeguard all individuals involved.

14. Publishing Students' Images and Work

Upon a student's enrolment, parents/carers will be asked to provide consent for the use of their child's images and work in the following contexts:

- On the academy website.
- On the academy's Learning Platform/VLE.
- In the academy's prospectus and other printed publications that the academy may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the academy's communal areas.
- In display material that may be used in external areas e.g., an exhibition promoting the academy.
- In general media coverage, including local or national press releases (distributed via traditional or electronic means)

This consent remains valid for the duration of the student's time at the academy unless circumstances change (e.g., changes in parental responsibility or custody arrangements). Consent may be withdrawn at any time by the person with parental responsibility, in writing.

To safeguard students' privacy:

- Full names will not be published alongside images.
- Email and postal addresses of students will not be disclosed.
- Prior to publishing student work online, staff must confirm that appropriate consent has been obtained.
- No images may be uploaded to websites or publications without prior approval from the Principal or a designated responsible person.

Only the White Rose Academies Trust or an authorised representative may upload images to official platforms. Where external links (e.g., YouTube) are used, a disclaimer must be included stating that the Trust is not responsible for the content of external sites.

15. Data Protection

When storing personal data on mobile or removable devices, the following safeguards must be in place:

- Data must be encrypted and password protected
- Devices must be secured with passwords and up-to-date antivirus/malware protection
- Data must be securely deleted once transferred or no longer required, in line with academy policy

Staff responsibilities include:

- Ensuring the safe handling of personal data to minimise risk of loss or misuse
- Recognising and reporting potential data breaches promptly
- Supporting data subjects in understanding their rights and handling requests appropriately
- Using only encrypted and password-protected devices for storing/transferring personal data
- Avoiding the transfer of academy data to personal devices unless explicitly permitted
- Accessing personal data only on secure, password-protected systems and logging off after use

16. Clear Screen Policy

To maintain data security:

- Users must log off from PCs/laptops when leaving them unattended for extended periods or overnight
- When stepping away from their desk, users should lock their screen using Ctrl + Alt + Del and selecting Lock Workstation
- WRAT devices may automatically lock after 15 minutes of inactivity, but manual locking is expected.
- Mobile devices (e.g., iPads) must be PIN protected, set to power off after five minutes of inactivity, and switched off when unattended
- Devices must be stored securely when not in use, including when working remotely

17. Monitoring Arrangements

The Trust and its academies employ a range of monitoring strategies to safeguard students and staff on internet-connected devices:

- Physical monitoring by staff observing screens
- Live supervision via device management consoles
- Network monitoring using logs of internet traffic and web access

- Individual device monitoring through software or third-party services

Monitoring systems must record:

- Source IP address
- Date and time of access
- Protocol used
- Destination site/server
- Where possible, the User ID initiating the traffic

Internet usage records are retained for 180 days. WRAT staff may access monitoring data to investigate security incidents. Reports identifying specific users, sites, or devices will only be shared externally upon written request and in accordance with GDPR principles.

Smoothwall alerts for online safety incidents are automatically sent to designated staff, including the DSL, DDSL, IT Manager, and Director of Safeguarding. All student-related incidents are logged and actioned via CPOMS.

Concerns regarding staff conduct must be reported to the relevant Principal, DSL, Director of Safeguarding, and HR.

This policy is reviewed annually by the Trust Executive Principal, Director of Safeguarding, Director of IT, Director of Governance, Principals, and academy DSLs. It is then shared with the Local Advisory Board (LAB).

18. Managing Email

The White Rose Academies Trust (WRAT) email system must be used responsibly and professionally. It must not be used to create, share, or forward any disruptive, discriminatory, or offensive content, including but not limited to comments related to race, gender, disability, age, sexual orientation, body image, religion, political beliefs, pornography or any content deemed to be illegal.

Any staff member or student who receives such content must report it immediately to the Designated Safeguarding Lead (DSL). Breaches of this policy may result in disciplinary action, including termination of employment or student exclusion, in accordance with WRAT's disciplinary procedures

The following practices are prohibited:

- Sending chain letters, joke emails, or mass mailings without IT approval
- Creating rules to automatically forward emails outside the WRAT domain, or using personal email accounts for WRAT business.
- Expecting privacy in communications sent via WRAT systems, emails may be monitored without prior notice

All email use must comply with the Trust's Acceptable Use Policy and safeguarding protocols.

19. Remote Learning

In exceptional circumstances where remote learning is authorised (e.g., school closures), staff must follow DfE guidance to ensure the safety and wellbeing of students and staff during online education

https://www.gov.uk/guidance/safeguarding-and-remote-education

Key expectations include:

- Using secure platforms approved by the Trust
- Maintaining professional boundaries and safeguarding protocols
- Ensuring students know how to report concerns
- Risk-assessing all remote learning tools and resources
- Following the school's behaviour and safeguarding policies during remote sessions

Staff must remain vigilant to signs of online abuse and report concerns promptly

20. Training

All staff receive online safety training during induction, with annual refreshers and updates via CPD, bulletins, and meetings. Training includes:

- Cybersecurity best practices (e.g., phishing awareness, device security)
- Risks of online abuse, including peer-on-peer abuse, cyberbullying, and radicalisation
- Recognising and responding to signs of online harm
- Supporting students in making safe and informed online choices
- Identify and challenge harmful online attitudes
- Ensuring students understand the importance of consent, respect, and kindness in digital interactions

- Recognise fake or AI-generated social media accounts and exaggerated online language
- Build resilience and critical thinking in the face of online misinformation

21. School Websites

School websites are a key public-facing platform and must comply with DfE statutory requirements. The Trust Marketing Team is responsible for ensuring content is accurate, up-to-date, and legally compliant.

Staff submitting content must:

- Credit all sources and respect copyright law
- Use only licensed or public-domain materials
- Avoid using content found via Google or YouTube without verifying copyright permissions
- Ensure it respects copyright and licensing laws. Permission must be obtained for any third-party content, and sources must be cited.

If in doubt, staff must consult the Trust Data Protection Officer before publishing.

22. Social Media Presence

Online Reputation Management (ORM) is essential to safeguarding the Trust's digital footprint. WRAT's Marketing Team oversees all official social media accounts (e.g., X/Twitter, Facebook, LinkedIn) and monitors online mentions, reviews, and Wikipedia entries. WRAT's social media accounts (e.g., Facebook, X/Twitter, LinkedIn) to:

- Promote Trust and academy achievements.
- Monitor public perception and feedback.
- Respond to legitimate public enquiries in a professional manner.

All public communication through these channels must reflect WRAT's values, comply with safeguarding obligations, and avoid bringing the Trust into disrepute.

All staff must adhere to WRAT's social media policy, which prohibits:

- Inappropriate interactions with students or families
- Sharing confidential or sensitive information
- Posting content that could damage the Trust's reputation

Concerns about staff conduct online must be reported to the Principal, DSL, Director of Safeguarding, and the WRAT HR TEAM.

23. Misuses or Infringements

All users of WRAT IT systems must be aware of how to report accidental access to inappropriate or harmful content. Such incidents must be logged immediately and reviewed by the appropriate safeguarding lead.

Staff: Any breach involving an adult working for WRAT (including central staff) must be reported directly to the Principal or the Trust's Director of Safeguarding. These incidents are to be documented in a centralised safeguarding log.

Students: Breaches by students will be handled in line with the school's Positive Relationships/ Behaviour Policy and Acceptable Use Policy (AUP), and recorded on CPOMS as a cause for concern. Designated Safeguarding Leads (DSLs) must categorise and action the incident appropriately.

All online safety incidents must be reviewed at least half-termly to identify trends, inform staff training, and shape preventative curriculum measures.

Sanctions will be applied proportionately, based on the severity and context of the breach.

Staff misuse of school systems, or inappropriate use of personal devices, will be investigated in accordance with the staff disciplinary policy. In serious or unlawful cases, WRAT will refer the matter to external agencies, including the police or the Local Authority Designated Officer (LADO) where required.

The Trust recognises its responsibilities under the Online Safety Act 2023 and will act accordingly where illegal or harmful online content is involved.

24. Personal Social Media Use by Staff, Students and Parents

All members of the school community are expected to uphold the highest standards of behaviour online, in line with the AUPs and professional conduct expectations.

Expectations:

- **Positive Engagement:** Posts must not be defamatory, aggressive, or discriminatory, nor should they bring the Trust or profession into disrepute.
- **Staff Conduct:** Staff must not discuss school matters or stakeholders on personal social media and should enable strict privacy settings. They must not accept or request online connections with students.
- **Student Conduct:** Students must not attempt to contact staff via social media. Such attempts must be reported as a safeguarding concern.
- **Parental Engagement:** Complaints or concerns should be raised directly with the academy. Social media is not an appropriate forum and can harm staff wellbeing and school reputation.

Age-Appropriate Use:

Parents are reminded of age restrictions on platforms (e.g., 13+ for most, 16+ for WhatsApp) and are encouraged to supervise their children's use of apps, games, and websites.

The academy recommends:

- Open conversations about children's online activity.
- Limiting unsupervised screen time, especially at night.
- Avoiding digital devices in bedrooms.

Communication Channels:

- The official channels for parent-school communication are email and direct contact with the academy.
- Social media platforms are not monitored for individual concerns and are not appropriate for child-specific communication.

Exceptions to professional boundaries (e.g., pre-existing family relationships) must be declared and approved by the Principal.

25. Bring Your Own Device

In cases where staff, students or others conducting business on behalf of the WRAT choose to bring their own device to one of our academies, they must refer to and follow the Trust's Bring Your Own Device policy.

26. Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Positive Relationships/Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints policy
- WRAT Employee Code of Conduct
- WRAT Bring Your Own Device Policy

Appendix 1 - ACCEPTABLE USE AGREEMENT – KS1

I understand that I must use the academy computer systems in a responsible way, to ensure that there is no risk to my safety, nor to the safety and security of the academy and other users.

Each time I log into the academy network I agree to the following rules:

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet for a while even if it was something I did outside of school.
- All the messages that I send people will be polite and kind.
- I will not share my password with anyone else.

Please complete the sections below to show that you have read, understood, and agree to this Acceptable Use Agreement.

If you do not sign this agreement, access cannot be granted to academy computer systems.

I have read and understand the above and agree to follow these rules when I use the academy computer systems and devices, both in and out of school.

STUDENT:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy).

SIGNATURE:
PRINT NAME:
DATE
PARENT*:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy). I have discussed it with my child, so they are aware of their responsibilities.

SIGNATURE:
PRINT NAME:
DATE:

*The term parent includes any person or body with parental responsibility, such as a foster parent, carer, guardian, or local authority.

Appendix 2 - ACCEPTABLE USE AGREEMENT – KS2

I understand that I must use the academy computer systems and any personal devices (including mobile phones) in a responsible way, to ensure that there is no risk to my safety, nor to the safety and security of the academy and other users.

Each time I log into the academy network I agree to the following rules:

I will keep myself safe by:

- Keeping my username and password secure and not sharing it.
- Not giving personal details about myself online (including address, phone number and date of birth).
- Reporting to an adult any inappropriate messages or anything online that makes me feel uncomfortable.
- Understanding the academy will monitor my use of the academy computers, email and internet.

I will treat others with respect, including:

- Being polite when I communicate online, not using aggressive or inappropriate language.
- Not taking or distributing images or videos of anyone without their permission.
- Making sure that my mobile phone (or other personal device, e.g. smart watch) is switched to silent and is handed in.
- Not touching another person's computer when they are logged in, especially not to log that user off.
- Not accessing, removing or altering anybody's files without their permission.
- Acknowledging the work of others to avoid plagiarism or copyright infringement.
- Not posting anything bad about the White Rose Academies Trust or any of their academies or their staff via social media or any other means.
- Not inviting teachers or staff to be a contact on social networking sites.

I will keep the academy computer systems safe and secure by:

- Not clicking on any links or attachments in emails unless I know the person they have come from (to prevent phishing or malware attacks).
- Not attempting to bypass the filtering or security systems in place.
- Not uploading / downloading programs nor anything illegal or inappropriate (e.g. defamatory, obscene or might cause distress to others).
- Reporting to an adult any equipment faults and not attempting to fix faults myself.
- Using OneDrive to store my files so I do not have to use portable media (e.g. USB memory sticks) within the academy.
- Understanding that the academy computer systems are for educational use only.

I understand that I am responsible for my actions both in and out of the academy:

- The academy has the right to act against me if I am involved in any inappropriate behaviour (covered in this agreement) when I am out of school if it involves students or staff from the academy.
- If I break this Acceptable Use Agreement, I will be disciplined, and I may not be allowed continued use of the academy computer system.

- If I am involved in any illegal online activity the academy will have to inform the police.

Please complete the sections below to show that you have read, understood, and agree to this Acceptable Use Agreement.

If you do not sign this agreement, access cannot be granted to academy computer systems.

I have read and understand the above and agree to follow these rules when I use:

- The academy computer systems and devices, both in and out of school.
- My own personal devices in the academy (if permitted).
- My own personal devices out of the academy (if it involves students or staff from the academy).

STUDENT:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy).

SIGNATURE:
PRINT NAME:
DATE:
PARENT*:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy). I have discussed it with my child, so they are aware of their responsibilities.

SIGNATURE:
PRINT NAME:
DATE:

* The term parent includes any person or body with parental responsibility, such as a foster parent, carer, guardian, or local authority.

Appendix 3 - ACCEPTABLE USE AGREEMENT - KS3/4

I understand that I must use the academy computer systems and any personal devices (including mobile phones) in a responsible way, to ensure that there is no risk to my safety, nor to the safety and security of the academy and other users.

Each time I log into the academy network I agree to the following rules:

I will keep myself safe by:

- Keeping my username and password secure and not sharing it.
- Not giving personal details about myself online (including address, phone number and date of birth).
- Reporting to an adult any inappropriate messages or anything online that makes me feel uncomfortable.
- Understanding the academy will monitor my use of the academy computers, email and internet.

I will treat others with respect, including:

- Being polite when I communicate online, not using aggressive or inappropriate language.
- Not taking or distributing images or videos of anyone without their permission.
- Making sure that my mobile phone (or other personal device, e.g. smart watch) is switched to silent and out of sight during the school day.
- Not touching another person's computer when they are logged in, especially not to log that user off.
- Not accessing, removing or altering anybody's files without their permission.
- Acknowledging the work of others to avoid plagiarism or copyright infringement.
- Not posting anything bad about the White Rose Academies Trust or any of their academies or their staff via social media or any other means.
- Not inviting teachers or staff to be a contact on social networking sites.

I will keep the academy computer systems safe and secure by:

- Not clicking on any links or attachments in emails unless I know the person they have come from (to prevent phishing or malware attacks).
- Not attempting to bypass the filtering or security systems in place.
- Not uploading / downloading programs nor anything illegal or inappropriate (e.g. defamatory, obscene or might cause distress to others).
- Reporting to an adult any equipment faults and not attempting to fix faults myself.
- Using OneDrive to store my files so I do not have to use portable media (e.g. USB memory sticks) within the academy.
- Understanding that the academy computer systems are for educational use only.

I understand that I am responsible for my actions both in and out of the academy:

- The academy has the right to act against me if I am involved in any inappropriate behaviour (covered in this agreement) when I am out of school if it involves students or staff from the academy.
- If I break this Acceptable Use Agreement, I will be disciplined, and I may not be allowed continued use of the academy computer system.

- If I am involved in any illegal online activity the academy will have to inform the police.

Please complete the sections below to show that you have read, understood, and agree to this Acceptable Use Agreement.

If you do not sign this agreement, access cannot be granted to academy computer systems.

I have read and understand the above and agree to follow these rules when I use:

- The academy computer systems and devices, both in and out of school.
- My own personal devices in the academy (if permitted).
- My own personal devices out of the academy (if it involves students or staff from the academy).

STUDENT:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy).

SIGNATURE:

PRINT NAME:

DATE:

PARENT*:

I have read, understood and agree to this Acceptable Use Agreement (further details can be found online in our Acceptable Use Policy). I have discussed it with my child, so they are aware of their responsibilities.

SIGNATURE:

PRINT NAME:

DATE:

* The term parent includes any person or body with parental responsibility, such as a foster parent, carer, guardian, or local authority.

Appendix 4 - Acceptable Use Agreement – Staff, Trustees, Governors and Volunteers

I understand:

- That I must use academy IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with children and young people.

- That portable media has many risks that could bring the academy, and Trust, into disrepute. Under no circumstances should any sensitive data files be stored on any portable media that is not encrypted. The White Rose Academies Trust takes the stance that USB portable media is unsupported due to the abundance of security risks. The Trust encourages all users to use Office 365 or SharePoint as a secure method of transferring files.
- That the Trust does not support the sharing of content on "Dropbox" or any other platform outside of the White Rose Academies Trust Office 365 ecosystem.
- If the Trust identify any illegal or concerning activity during monitoring (for example under the Child Protection Act, Radicalisation under the PREVENT Duty or Counter-Terrorism and Security Act) I will be referred as appropriate to statutory partners for investigation.
- That the data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.

Prevent – Due regard to the need to Prevent Staff from being drawn into Terrorism

There is an important role for White Rose Academies Trust in helping prevent people being drawn into terrorism. Terrorism which includes not just violent extremism but also non-violent extremism and radicalisation can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. It is a condition of funding that White Rose Academies Trust must comply with relevant legislation and any statutory responsibilities associated with the delivery of education and safeguarding of learners.

When using the WRAT's IT systems and accessing the internet in, or outside the organisation on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the reputation of the WRAT.

- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the WRAT's network using someone else's details.
- Take photographs/videos of students without getting written permission to do so first from a line manager.
- Share confidential information about the WRAT, any of its academies, its students or staff, or other members of the community.
- Access, modify or share data I am not authorised to access, modify or share. If I find I have access to data that I should not have access to, I will report it to the data owner or the IT department.
- Promote private businesses, unless that business is directly related to the WRAT, and with permission to do so.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not engage in any online activity that may compromise trust and confidence in my professional integrity, responsibilities, or bring the reputation of the WRAT into disrepute.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only communicate with students and parents/ carers using official academy systems. Any such communication will be professional in tone, manner and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or public chat/ social networking programmes must not be used and communication through these means may result in disciplinary action.
- I will immediately report any loss, or possible compromise of personal data, however this may have happened.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only use the WRAT's IT systems and access the internet in, or outside my organisation on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the WRAT will monitor the websites I visit and my use of the WRAT's IT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of work, and keep all data securely stored in accordance with this policy and the WRAT's data protection policy.
- I will let the designated safeguarding lead (DSL) and IT know if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

- I will always use the WRAT's IT systems and internet responsibly and ensure that students in my care do so too.
- I will ensure that I will abide by all safeguarding policy and procedures relating to the use of IT, including the WRAT Employee Code of Conduct and Guidance for safer working practices for professionals working in educational settings (NSRC, February 2022).

Signed:

Date: