Elm Tree Multi Academy Trust

Online Safety and Acceptable Use Policy

September 2026

Approval and Review
This Policy is reviewed in discussion with staff and governors. **Effective from**: September 2026 **Approved by**: Trust Board **Review date**: September 2027 **Review Leader: Trust Safeguarding Lead**

Table of Contents

1. Policy Aims 3
2. Legislation and guidance 3
3. Roles and Responsibilities 4
4. Implementing and Reviewing the Policy 6
5. Educating students about online safety 7
6. Educating parents / carers about online safety 8
7. Training 9
8. Staff Email and use of Social Networking Sites 9
9. Student Email 10
10. Filtering and Monitoring 10
11. How will Internet access be authorised? 11
12. Online Safety for students with additional needs 11
13. How will the school respond to any incidents of concern or misuse? 12
14. Cyber-Bullying 13
15. Examining Electronic Devices 14
16. Use of mobile devices in school 15
17. Shared Access Areas 15
18. How will the policy be communicated? 16
Annex 1: Acceptable Use Policy (AUP) for Staff 17
Annex 2: North Leamington School Acceptable Use Policy for Students 18
Annex 3: Telford Junior School Acceptable Use Policy for Pupils 19
Annex 3: Acceptable Use Policy for Visitors 20
Annex 4: Mobile Devices 21

1. Policy Aims

- To have robust processes in place to safeguard children, young people and staff
- To 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
- To identify roles and responsibilities and to recognise that online safety is a part of the duty of care which applies to everyone working with children
- To raise awareness of the importance of online safety with staff so that they are able to educate and safeguard children in their care
- To provide parents and carers with the opportunity to develop their knowledge of online safety

In line with the document *Keeping Children Safe in Education*, Elm Tree Multi Academy Trust is aware of their legal obligation to safeguard and protect children online and offline and the accountability of these decisions will sit with the Headteacher and the Governing Body.

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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **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) including those generated using AI, and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
- Mobile phones in schools

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle

cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

Trustees

Trustees will take overall responsibility for monitoring this policy and ensuring it meets the needs of all those within the Trust and ensure the policy is compliant with all regulation regarding the online safety within schools.

The governing board

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The governing body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared reporting system to make sure safeguarding concerns are received, monitored and acted on without delay.

The Trust Safeguarding lead will:

Take responsibility for monitoring and advising on our compliance with safeguarding requirements including in relation to online safety and the compliance with Keeping Children Safe in Education (KCSiE) 2026

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with the school's behaviour and child protection policy
- Updating and delivering staff training on online safety Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Behaviour and Engagement policy (available on our website)

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of online bullying are dealt with appropriately in line with the school's behaviour and engagement policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Implementing and Reviewing the Policy

1. The Online Safety Policy is written in conjunction with the Child Protection Policy, Anti-Bullying Policy and Behaviour and Engagement Policy. Schools will consult with staff, governors and students in creating the policy.

2. Each school's Designated Safeguarding Lead and the Deputy DSL is trained in supporting any child wishing to disclose information regarding an online incident. In their absence there are other members of staff who are appropriately trained by Warwickshire Safeguarding Children Board to appropriately support children in the event of a safeguarding concern.

3. All members of the school community are informed about the procedure for reporting online safety concerns, including breaches of cyberbullying, filtering and illegal content.

4. The school will manage incidents of online safety in accordance with our anti-bullying and behaviour policies where appropriate, and will engage parents / carers accordingly.

5. The Headteacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity. Our School Policy has been approved by governors.

5. Educating students about online safety

Students will be taught about online safety as part of our taught curriculum, and using guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach Relationships and sex education and health education in secondary schools

5.1 Children in Key Stage 2 will be taught to:

• Use technology safely, respectfully and responsibly.

• Recognise acceptable and unacceptable behaviour.

• Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

• That people sometimes behave differently online, including by pretending to be someone they are not.

• That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.

• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

• How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met.

• How information and data is shared and used online.

• What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

• How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

• How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant. In

Children in Key Stage 3 will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

5.2 Children in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5.3 Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.
All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive appropriate age education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

6. Educating parents / carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents and carers.

The school will inform parents and carers:

- What systems the school uses to filter and monitor online use
- What their children are learning about online safety

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Year Leader and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Deputy Headteacher.

7. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and their deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

8. Staff Email and use of Social Networking Sites

- All staff will be provided with a school email account. The email system is not to be used for the creation or distribution of any type of offensive or disruptive content. If staff receive any messages of this type, then they must report it to the Designated Safeguarding Lead. If offensive or disruptive content is received from another member of staff, then this must be reported to the Headteacher.

- In the school context (as in the business world), email should not be considered private, and schools reserve the right to monitor email. Staff understand they must use a work provided email account to communicate with parents/carers, students and other professionals for any official school business. This is important for confidentiality and security, and also to safeguard members of staff. If a

member of staff is found to be in breach of the email policy rules this could result in disciplinary action.

- Parents, carers and staff need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

- Staff should ensure that their personal social network pages are sufficiently protected to minimise any parents or students to access personal information, comments or photographs. It is recommended that Facebook security and privacy settings are set to 'Friends Only' thus preventing them being viewed by the general public.

- Staff must not accept current students on roll as friends on any form of social media. This is in line with the Staff Behaviour Policy.

- Staff should not use social networks sites or the internet or personal blogs etc. in such a manner that the content is derogatory towards colleagues or brings the school into disrepute.

- School respects a staff member or student's right to a private life, but it must also ensure that confidentiality and its reputation are protected. It therefore requires staff and students using social networking websites to:

  - refrain from placing any work-related issue or material that could identify an individual who is a student or colleague, which could adversely affect the school
  - ensure that they do not conduct themselves in a way that is detrimental to the school
  - take care not to allow their interaction on these websites to damage working relationships between colleagues and students

9. Student Email

a) Students may only use school provided email accounts for school purposes.
b) Students must immediately tell the Designated Safeguarding Lead if they receive offensive email.
c) Students must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
d) The forwarding of chain messages is not permitted.

10. Filtering and Monitoring

- Access controls fall into several overlapping types (commonly described as filtering):
  a) Filtering is provided by a Smoothwall appliance. This curates lists of websites in various categories such as Education, Video, Gaming etc, based on their content and key words.
  b) Users are assigned to groups based on their age, position in the school courses taken or taught. These groups are granted access to different categories of sites.
  c) Sites that defy grouping will be added or removed by the IT team.
  d) Monitoring is provided by Smoothwall's RADAR software which is managed by Warwickshire Education Systems team (WES).
  e) RADAR monitors every word displayed on screen and takes screen shots when key words appear which may suggest that a staff member or student is vulnerable. These screen shots are notified to schools and subsequently investigated accordingly.

- Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the school's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access.

- Websites which staff and students believe should be blocked centrally should be reported to the ICT Helpdesk. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Extra care must be taken with any resource that allows public comments as these can contain unsuitable material.

a) The school's broadband access includes filtering appropriate to the age and maturity of students.
b) Each school within the Trust has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure.
c) Each school's filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
d) Changes to the school's filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
e) The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
f) Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Warwickshire Police or CEOP in line with Child Protection procedures.
g) Each school's curriculum will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

11. How will Internet access be authorised?

Each school should allocate Internet access to staff and students on the basis of educational need and withholds the right to withdraw access following any concerns which identify a risk to themselves or other staff / students whilst accessing school devices.

a) All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
b) Parents will be asked to read the School Acceptable Use Policy for students (Annex 2) and discuss it with their child, where appropriate.
c) All visitors to the school site who require access to the school's network or internet access will be required to read and sign an Acceptable Use Policy.
d) Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.
e) When considering access for vulnerable members of the school community (such as for children with special education needs) the school will make decisions based on the specific needs and understanding of the student(s).

12. Online Safety for students with additional needs

- Elm Tree Multi Academy Trust has due regard for the Equalities Act (2010) and is guided by the Special Educational Needs and Disabilities Regulations (2014). It is recognised that students may have individual needs that will present different issues when teaching about the risks and impacts associated with online safety. Some students may be still developing their social understanding of safety and so may require reasonable adjustments to be made when considering strategies to educate them about online safety.

- The school SENDCO will coordinate advice between teaching and support staff. This should take the form of student focused strategies that would apply to a student with specific needs that would need to be available to all staff implicated in Internet use with that student.

13. How will the school respond to any incidents of concern or misuse?

- Where there is cause for concern that illegal activity has taken place or is taking place involving the use of computer equipment, schools will determine the level of response necessary for the offence disclosed, in line with the school's policies on behaviour and ICT Acceptable Use.
- Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff behaviour (code of conduct) policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

- The facts of the incident or concern will need to be established, and evidence should be gathered where possible and appropriate. Online incidents may have an impact on students, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

- A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious, and a range of sanctions may then be required, which are linked to the school's relevant Behaviour Policy. Potential child protection or illegal issues must be referred to the school Designated Safeguard Lead. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

a) All members of the school community will be informed about the procedure for reporting online concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
b) All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
c) Any complaint about staff misuse will be referred to the Headteacher. Or the chair of the governors if the complaint relates to the Headteacher
d) An appropriately trained member of staff will record all reported incidents and actions taken in the student e-portfolio and in any relevant areas e.g. Bullying or Child protection log.
e) The Designated Safeguarding Lead will be informed of any online incidents involving Child Protection concerns, which will then be escalated appropriately in accordance with the Child Protection Policy.
f) The school will manage online incidents, including sanctions, in accordance with the student Behaviour Policy, or staff Code of Conduct where appropriate.
g) The school will inform students and parents/carers of any incidents of concern and procedures followed as and when required. Schools ask for parents to work in partnership with school to resolve issues identified.
h) After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
i) Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or escalate the concern to the Police
j) All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

14. Cyber-Bullying

This policy should be read in conjunction with the school's Anti Bullying Policy.

14.1 Definition

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone." (DfE, 2007). Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour / anti-bullying policies.)

14.2 Preventing and addressing cyber-bullying

- Headteachers have the ability to implement the school's Behaviour policy when they are not on school premises or under the lawful control of school staff; this may be as the result of an online incident having offline consequences.

- Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on where reasonably practicable.

- Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feel that an offence may have been committed, this will be referred to the Police.

- The NSPCC, Think You Know and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying.
  a) Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and Engagement for Learning.
  b) There are clear procedures in place to support anyone in the school community affected by cyberbullying.
  c) All incidents of cyberbullying reported to the school will be recorded.
  d) There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
  e) Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
  f) The school will take steps to identify the perpetrator where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
  g) Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online ethos.
  h) Sanctions for those involved in the misuse of school systems:
     i. The perpetrator will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the perpetrator refuses or is unable to delete content.
     ii. Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance with the schools Anti-bullying Policy, Engagement for Learning Policy or Acceptable Use Policy.
     iii. Parent/carers of students will be informed.
     iv. The Police will be contacted if a criminal offence is suspected.

15. Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or 7 files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Each school's Behaviour policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Therefore, the Headteacher, and any member of staff authorised to do so by the Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to DSL or to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with our behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Elm Tree Multi Academy Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Our schools will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with schools' AI usage policy.

16. Use of mobile devices in school

In line with statutory guidance, our schools are mobile phone-free environments by default. [1] Please refer to Annex 4 for individual schools' arrangements.

17. Shared Access Areas

a) SLT and staff will regularly monitor the usage of shared areas by students and staff, in particular message and communication tools and publishing facilities.
b) Students/staff will be advised about acceptable conduct and use when using the school shared areas
c) Only members of the current student, parent/carers, staff community and occasionally authorised guests will have access to the school's shared areas.
d) All users will be mindful of copyright issues and will only upload appropriate content onto shared areas of the school's network.
e) When staff and students leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
f) Any concerns about content on the school's shared areas may be recorded and dealt with in the following ways:

[1] https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools

i. The user will be asked to remove any material deemed to be inappropriate or offensive.
ii. The material will be removed by the site administrator if the user does not comply.
iii. Access to the school's network may be suspended for the user.
iv. The user will need to discuss the issues with a member of SLT before reinstatement.
v. A student's parent/carer may be informed.

g) This guidance should be read in conjunction with the Staff Code of Conduct and the Acceptable Use Policy.

18. How will the policy be communicated?

59. Consideration is given as to the curriculum place for teaching online safety, and the contents of this policy through curriculum learning.

a) This policy is available on the ETMAT schools' websites
b) To protect staff and students the school has implemented an Acceptable Use Policy
c) The Online Safety policy is provided to all members of staff on induction and discussed as part of our staff training programme
d) A partnership approach to online safety at home and at school is be encouraged by offering parental online safety sessions with school and external agencies.
e) Regular training is be provided to staff to inform them of the contents of this policy
f) All users are informed that network and Internet use will be monitored.
g) Online Safety training is be delivered across the school to raise the awareness and importance of safe and responsible internet use amongst students.
h) Student instruction regarding responsible and safe use precedes students being given access to the Internet.
i) Online Safety lessons are included in the PSHE, Tutor Time and/or ICT programmes covering both safe school and home use.
j) Online training is part of the transition programme across the Key Stages and when transitioning from Primary School.
k) Safe and responsible use of the Internet and technology is be reinforced across the curriculum and subject areas.
l) Particular attention to online education is given where students are considered to be vulnerable.

Links with other policies

- Child Protection Policy
- Anti-Bullying policy
- AI Policy
- Behaviour Policy / Suspension and Permanent Exclusion Policy
- Staff Code of Conduct
- Data Protection Policy
- Mobile Phone Policy

Annex 1: Acceptable Use Policy (AUP) for Staff

This AUP is to be read in conjunction with the Staff Code of Conduct and the Child Protection Policy.

It is understood and accepted that all use of computer resources provided by the school is monitored and can be reported upon at any time for Safeguarding and Management purposes.

1. Staff should not expect privacy of personal communications while using computers or communications technologies provided by the school and agree that such communications may be monitored and subject to review.
2. Staff must use communications technologies, e.g. mobile phones, email accounts, provided by the school to communicate with children and their parents/carers, making sure that parents/carers have given permission for this form of communication to be used.
3. Staff must not share personal contact details with students.
4. Staff must only make contact with children for professional reasons and in accordance with the Code of Conduct and other school policies.
5. Staff must ensure that privacy settings are set at maximum on any social networking sites they use and that students and their parents/carers are never able to view the content or listed as approved contacts.
6. Staff must never use social networking sites to contact students currently on roll
7. Staff must not transmit confidential, sensitive, or personally identifiable information outside of the school network without following policy-approved security procedures.
8. Online conduct of staff must not bring the good standing of the school into disrepute.
9. Staff will refrain from using their mobile devices in student facing areas and in the presence of students unless in the event of an emergency.
10. Use any improper language when communicating online, including in emails or other messaging services

Annex 2: North Leamington School Acceptable Use Policy for Students

The use of the computers and internet at North Leamington is granted by the school to students with the understanding that they will follow the school's rules and the law. This is to keep students in our school community safe.

If you do not adhere to these rules, then access to the computers or internet at North Leamington School may be withdrawn in line with the school's Behaviour and Engagement Policy.

If you use the computers or internet at North Leamington School, you are agreeing to these rules:

- School computers and networks are always monitored to keep children and adults safe
- Users are responsible for all activity on their device or user account
- Users should not provide their date of birth, personal address or contact number, or the date of birth, personal address or contact number of other users
- Users should not share images of themselves or anyone else
- Be polite and use appropriate language. Do not swear or use vulgarities. Do not harass or intimidate
- Users must not use someone else's username or attempt to access another user's account
- Users must not write down their password, or share their password with another user
- Users must not try to break or hack the network
- Users must not use the network or their own device to access pornography, inappropriate text files, or anything else that is not appropriate in school or illegal
- Users must not attempt to bypass the school's internet by using VPNs or other mechanisms to access the internet
- Users must not break the copyright on films, music, images and etc
- Users must report any unpleasant material or message sent to them to an adult. This report will help protect other users
- If a user infringes the above rules, their account may be inspected and their access withdrawn. Their Year Leader and parents will be informed of any rules that are broken
- Whilst on school site, students are not permitted to access the internet except through the school network
- Students are not permitted to use mobile phones or other electronic devices (including tablets, ear buds, gaming devices) whilst on site. If devices are seen by staff members, then they will be confiscated and this will be recorded as a behaviour incident.
- In some situations, mobile devices may be permitted for individual students with relevant permissions, or for the purpose of teaching and learning, under close supervision by teaching staff.
- Users must adhere to the school's AI Acceptable Use principles, including the principles of:
    - The use of AI for research and study support
    - Data protection
    - The use of AI for classwork and internal assessment
    - The use of AI in formal assessments including NEAs and externally set assignments
    - The ethical and appropriate use of AI

Annex 3: Telford Junior School Acceptable Use Policy for Pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only. • Only use them when a teacher is present, or with a teacher's permission. • Keep my username and passwords safe and not share these with others. • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer. • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. • Always log off or shut down a computer when I'm finished working on it. I will not: • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Log in to the school's network using someone else's details. • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. I will not bring a personal mobile phone or other personal electronic device into school, unless under very specific circumstances and with the expressed permission of the school staff and my parents/carers. My parents/carers will have had to make such an arrangement with the school. I would then be required to hand the mobile device to the school office during the school day. I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	

Annex 3: Acceptable Use Policy for Visitors

This Policy is a guide to the acceptable use of the school's Guest Wireless network facilities and services.

Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use Policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

Occasionally, our schools will provide a guest wireless network to our visitors. This network is provided on a best endeavours basis and as such we cannot guarantee that it will be available or secure.

It is understood and accepted that all use of computer resources provided by the school is monitored and can be reported upon at any time for Safeguarding and management purposes.

The school takes no responsibility and assumes no liability for any content that may be lost or compromised while connected to the Guest Wireless Network.

North Leamington School reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to the school's intranet or permission to install any software on our computers.

Inappropriate use of the Guest Wireless Network is not permitted. This policy does not cover all possible inappropriate uses but rather presents some guidelines (listed below) that Elm Tree Multi Academy Trust may at any time use to make a determination that a particular use is inappropriate:

- Users must respect the privacy and intellectual property rights of others.
- Users must respect the integrity of our network and any other public or private computing and network systems.
- Use of the Guest Wireless Network for malicious, fraudulent, or misrepresentative purposes is prohibited.
- The Guest Wireless Network may not be used in a manner that precludes or hampers other users access to the Guest Wireless Network or other any other networks.
- Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.
- Visitors will refrain from using their mobile devices in student facing areas and in the presence of students unless in the event of an emergency.

Annex 4: Mobile Devices

North Leamington School

In line with statutory guidance, our school is a mobile phone-free environment by default. Students are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by senior staff.

Where there is an arrangement by exception, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see annex 2 and 3). Any breach of the acceptable use agreement by a student may trigger a sanction in line with the school behaviour policy, which may result in the confiscation of their device.

Sixth-form students may be permitted access to their mobile phone at certain limited times and locations (e.g. in a sixth-form common room). Sixth-form students remain subject to the school's behaviour policy and misuse of their phone may lead to sanctions pursuant to the school's behaviour and mobile phone policies.

We recognise that children may need to have mobile devices in their possession to access when on the way to/from school. However, North Leamington School is a 'no mobile phone' site for years 7-11. This also includes any other mobile, internet enabled, SMART or electronic devices such as tablets, headphones or digital cameras, unless approved by staff members in advance. Members of the Sixth Form are permitted to use their mobile phones in permitted areas; however no Sixth Form student is permitted to have their phone on show in the presence of younger students. To uphold the importance of this policy we also ask that staff members do not access their mobile phones in the presence of students or in student facing areas.

Should a student have their mobile phone or device seen by a member of staff, our procedures are outlined in the confiscation process.

- Mobile phones, or other electronic devices, could lead to child protection/safeguarding and data protection issues with regard to inappropriate capture or distribution of images of students or staff
- Mobile phone usage can render staff or students subject to Cyberbullying
- Internet access on mobile devices cannot be filtered by the school
- Inappropriate use of mobile devices can undermine classroom discipline and distract teaching and learning.
- If mobile devices are used as part of authorised learning activities, then the school will provide Wi-Fi codes on a controlled and time specific basis so that our monitoring systems protect students' use

In some situations, mobile devices may be permitted for individual students with relevant permissions, or for the purpose of teaching and learning, under close supervision by teaching staff.

Telford Junior School

As a primary school, pupils should not bring mobile devices into school (e.g. mobile phones, smartwatches, etc.). In exceptional cases, parents/carers may ask for their child to have a mobile device on them when travelling to and from school (e.g. if a child is using public transport). This should be agreed with the school (class teacher / head teacher) and the device should be handed into the school office during the school day.