

Online Safety Procedure

Thomas Russell Infants



This procedure should be read in conjunction with the JTMAT Safeguarding Policy

Approved by: LGB

Date: 26/9/2023

Last reviewed on: 17/09/2023

Next review due by: September 2024

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	4
5. Educating parents about online safety	5
6. Cyber-bullying	5
7. Sharing nude and semi-nude images	5
8. Acceptable use of the internet in school	7
9. Pupils using mobile devices in school	7
10. Staff using work devices outside school	8
11. How the school will respond to issues of misuse	8
12. Training	8
13. Filtering and Monitoring arrangements	9
14. Links with other policies	11

.....

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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
- 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, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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](#) – remove if not applicable, see section 4]
- > [Searching, screening and confiscation](#)

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](#) 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.

The policy also takes into account the National Curriculum computing programmes of study.

Non-statutory guidance from the Department for Education on sharing nude and semi-nude images is available [here](#) and is used to support section 7 of this procedure.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this procedure and holding the Head of School to account for its implementation.

The Designated Safeguarding Lead (DSL) will provide data to the Governing Body as part of the Head's Report on a half termly basis. Online Safety discussions will take place between the DSL and Safeguarding Link Governor.

All governors will:

- Ensure that they have read and understand this procedure
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (<http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf2>)

3.2 The Headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) **and deputies** are set out in our safeguarding procedure.

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

- Ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the IT Technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying and online abuse are logged and dealt with appropriately in line with the school behaviour procedure
- Delivery of online safety information through Safeguarding CPD programme and Safeguarding updates
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 The Senior IT Technician

The IT Technician is responsible for:

- Monitoring and maintaining appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this procedure
- Implementing this procedure consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (<http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf>).
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this procedure.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this procedure
- Read and utilise the information available on the school website to promote Online Safety at home.
- Monitor their child's use of social media and ensure they are safe when using the internet.
- Monitor their child's mobile device and online activity, particularly in reference to online hoax material and online challenges.
- Use social media communications appropriately and positively, especially when making reference to the school or staff specifically, avoiding situations where negative or derogatory comments are posted in the public domain.

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](#)
- › [Healthy relationships – Disrespect Nobody](#)

3.7 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 procedure, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use <http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf>.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

Key stage 1

Pupils should be taught to:

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

By the **end of primary school**, pupils will know:

Online relationships

- 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

All teachers are responsible for ensuring that teaching and delivery is adapted to meet the needs of their students, including those with SEND and those who are vulnerable.

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents 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 procedure will also be shared with parents via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a member of the Safeguarding Team.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. 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 procedure.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding updates.

The school also has information links available on the website to support parents and carers with Online Safety.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour procedure. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 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 files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material (under supervision of a member of staff/parent/carer), or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Where inappropriate material has been reported, found or suspected staff will contact parents/carers who will be required to collect the device from school.

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

7. Sharing nudes and semi-nude images.

Sexting is defined in our Whole School Policy for Safeguarding Incorporating Child Protection which can be found here. <https://jths.co.uk/policies-and-procedures>

Non-statutory advice from the Department for Education is available to support education settings, this advice can be found here.

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people#annexa>

This guidance will be used in conjunction with this procedure and the JTMAT Whole School Policy for Safeguarding.

7.1 Information for Staff responding to concerns regarding nude and semi-nude images

- Staff MUST follow the Safeguarding referral process as outlined in the JTMAT Safeguarding Policy.
- Concerns related to nude and semi-nude images MUST be reported to the DSL or Deputies.
- Staff MUST NOT ask to see/view any images or videos

7.2 Information for Safeguarding staff responding to concerns regarding nude and semi-nude images

- Speak to the child/children/young person
- Involve parents/carers
- Determine the classification using fig 1 from the DfE Guidance
- Determine if a referral to Social Services or the Police is appropriate NOTE: there is clear guidance in relation to contact with the Police and criminalization of children in the DfE Guidance.

7.3 Supporting the child/children/ young person

- Establish if the image has been shared
- Ensure the content has been deleted, supervised by a member of staff or parent/carer
- If the image has been shared signpost the child/children/young person to Childline <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/>
- Establish if there are wider risks to the child/children/young person and consider a referral to an outside agency as appropriate.

7.4 Role of Parents/Carers

- Receive information and advice about the sharing of images
- Support your child/children to delete any inappropriate images, including from backups and cloud based storage.
- Support your child/children with contacting Childline to report and remove shared images <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/>
- Be aware of the law in relation to sharing materials
- Support school with consent to a referral to external agencies, where appropriate

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (<http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf>). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in <http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf>.

9. Pupils using mobile devices in school

Pupils are not permitted to bring personal devices to school. School laptops and ipads are used by pupils, under supervision and the use of these is monitored by our school, monitoring and filtering system

10. Pupils using school devices off site

All students who are loaned a school device will have to sign an additional agreement and consent form. Students/ Families are liable for costs associated with damage to loaned items.

Students using school devices should be made aware that they are monitored using our monitoring software, inappropriate use could result in pastoral or safeguarding follow up.

Students using school loaned devices should ensure they are not used for purposes other than education or by other members of the household.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in <http://resources.jtmat.co.uk/policies/ICTSecurity-AUP.pdf>.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT Technician.

Work devices must be used solely for work activities. Staff should be aware that all laptops and PCs are covered by our monitoring software.

12. Social Media

Thomas Russell Infants School has a Twitter account. This are identifiable as:

Twitter: @trisschool

We acknowledge that some individual staff and departments may choose to use social media as a way of communicating with our wider community in their professional capacity. Staff who do this must ensure that their activity and interactions online meet the expectations of the JTMAT Staff Code of Conduct. Personal activity on social media is also covered in the JTMAT Staff Code of Conduct.

Under no circumstances are any members of our school community permitted to create imitation or impersonation accounts online.

Our social media platforms are not formal methods of communication between stakeholders and school. We ask that you contact the School Office directly to raise any concerns.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Our monitoring software informs staff in school of 'Graded Captures' when they reach the threshold for Grade 4 or Grade 5 which would indicate a potential Safeguarding risk. When this is the case, students will be spoken to and parents will be informed. If there is evidence of misuse of ICT, then a follow up is likely to be implemented.

The school are also able to enforce the Behaviour for Learning and Behaviour Management procedure for incidents related to online abuse. Sanctions can include but are not limited to detentions, extended reflection, suspensions and permanent exclusions.

14. 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 pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The SSSCB Level 1 Training also highlights the risks around Online Safety.

The DSL and 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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Filtering and Monitoring arrangements

15.1 Roles and Responsibilities

All Staff

All staff are responsible for ensuring they are safe online and comply with the JTMAT Acceptable User Policy. All staff are responsible for reporting any concerns about online safety.

Student online safety concerns are reported via MyConcern.

Staff online safety concerns are reported to the Headteacher.

Concerns about filters, including allowing access and blocking access must be logged as a support ticket with the IT Team via the helpdesk.

Teaching Staff

Teaching staff using computer facilities around school are responsible for ensuring students are using the IT equipment and online facilities in a safe way.

Leadership Team

The SLT are responsible for ensuring that IT provision in school is adequately meeting the needs of staff and students, balancing the need for effective safeguarding, filtering and monitoring with providing high quality teaching and learning.

Governing Body

The Governing Body are responsible for ensuring that the school meet the requirements of KCSIE, 2023 and the published safety standards.

Designated Safeguarding Lead

The DSL has the lead responsibility for Online safety, filtering and monitoring.

Deputy Designated Safeguarding Leads

The DDSLs will support the day-to-day management of online safety referrals.

IT Support Staff

Are responsible for the day-to-day maintenance of the IT infrastructure and filtering in place on the school network.

Are responsible for running the filtering checks and sharing the reports with the DSL.

Are responsible for running a termly report on updated (added/removed) filters with reasons and sharing this with the DSL.

Are responsible for keeping a record of all tickets logged via the helpdesk related to filtering.

15.2 Filtering

There are multiple layers of filtering in place on the TRIS Network. The initial layer of filtering is done at source by the internet provider. This filters the most inappropriate material at source.

The Strategic ICT Lead for JTMAT is able to see all TRIS Filtering categories.

Filtering is then set up by user group. Student accounts and access is the most restricted across the school network.

Group 1- Students- Most restricted

Group 3- Staff

Group 5- Least restrictive for specialist users (staff)

Some filtering at source is padlocked, this means there is no control for school to adapt or edit the level of filtering.

The IT Support Staff are able to add additional filters on to ensure the safety of the materials being accessed by staff, students and visitors.

If staff require filters being removed to allow access to specific material, this can only be done in consultation with the DSL.

Filters apply to all devices that use the school network.

15.2 Monitoring

The school's IT system is monitored by Securus. This is a paid service that tracks keystrokes across all IT platforms including Microsoft Office, Online search engines and all other interfaces. The paid service review all captures by staff and students and assign them with a grading 1-5, with 5 being most significant.

The school is notified of all Grade 4 and Grade 5 captures via email. Staff and student captures are reported to the Headteacher.

All Grade 4 and Grade 5 captures are reported on MyConcern, even if they are false positives.

Securus provide a monthly report to the DSL and DDSL. Information will be discussed in DSL supervision meetings to support preventative education around any emerging patterns or trends related to Online Safety.

The DSL and Deputies log behaviour and safeguarding issues related to online safety. Online safety incidents are reported via MyConcern. All staff are responsible for monitoring online safety when using IT facilities in school and reporting student issues via MyConcern.

If the monitoring system flags harmful material that is not being filtered the DSL and DDSL will log this with the IT Support Staff to ensure access to these sites are removed.

All staff have a responsibility to log any unfiltered websites with the IT Support Staff where they believe access to this site would pose a risk to children. This must be logged by contacting the IT Help Desk via Email.

The IT Support staff will then record the action taken and keep a record of this.

Each term the DSL will review the filtering lists in school.

The IT Support staff are responsible for running a termly test on the Filtering in place and sharing this report with the DSL as part of the termly review process. This test is to check compliance with recommended safety standards.

In addition to the external monitoring, the IT Support Staff are able to track login information within school and externally, this can be done when school login information is used on school and personal devices.

This procedure will be reviewed annually by the DSL. At every review, the procedure will be shared with the governing board and staff.

16. Links with other policies

This Online Safety Procedure is linked to our:

- JTMAT safeguarding policy
- TRIS safeguarding procedure
- TRIS Behaviour Procedures
- JTMAT Staff Code of Conduct
- JTMAT Data protection policy and privacy notices
- JTMAT Comments, Compliments and Complaints procedure
- ICT Security- Acceptable Use Policy

