John Taylor Free School

Online Safety Procedure

This procedure should be read in conjunction with the JTMAT Online Safety Statement and the JTFS Safeguarding Policy.

Implementation Date:	January 2022
Review Date:	September 2024

Contents

1. Aims

Our school aims 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This procedure is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 students' electronic devices where they believe there is a 'good reason' to do so. 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 of School Report on a half termly bases. 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.

3.2 The Head of School

The Head of School 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 child protection and safeguarding policy.

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

- Supporting the Head of School in ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the Head of School, Senior 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 are logged and dealt with appropriately in line with the school behaviour procedure
- Delivery of online safety information through safeguarding E-Newsletters
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School and/or governing board This list is not intended to be exhaustive.

3.4 The Senior IT Technician

The Senior IT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students 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 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 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 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 Head of School of any concerns or queries regarding this procedure
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- 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: https://www.saferinternet.org.uk/advicecentre/parents-andcarers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In Key Stage 3, students 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 Students in

  Key Stage 4 and Key Stage 5 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

The safe use of social media and the internet will also be covered in other subjects where relevant.
Educating students in relation to online challenges and hoax material will be covered as part of the pastoral provision.
The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students 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 Head of School.

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 students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Tutor Time, Morning Registration and other subjects where appropriate.

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

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 students, 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 students' 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.)
- 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 students 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 students' 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.

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

This guidance will be used in conjunction with this procedure and the Safeguarding Policy.

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

- Staff MUST follow the Safeguarding referral process as outlined in the 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 or semi-nude images.

- Speak to the child/children/young person
- Involve parents/carers
- Determine the classification using fig1 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
- 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
- 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 students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

8.1 Monitoring of devices and activity online

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. All Windows devices (both student and staff) have Smoothwall Monitor installed which provides proactive real-time monitoring.

- The client captures user activity as it happens and automatically sends potential risks through to the Monitor portal and the safeguarding team are alerted instantly to any potential high risk alerts.
- Our Netsweeper Web Filtering allows us to have separate Staff and Student Filtering policies, therefore ensuring that suitable filtering levels are applied per user.
- Netsweeper provides dynamic categorization, therefore ensuring that all new websites are categorized appropriately.

Entrust Monitoring Service protects students from harmful content. It is a granular, content aware filtering service that reviews, monitors and tracks and notifies us of any safeguarding risks including radicalisation, suicide and self harm.

- This comprehensive protection software sends an immediate email to three assigned leads in school to alert concern and gives a graded capture.
- The three identified staff are:
  - Liz
  - Andrew Warner
  - Michelle Hassell
- When a graded capture is identified, the staff identified receive an alert email detailing the level of concern through the monitoring software. As a team in school we then identify user name and location, alongside viewing content which has raised concern.
- We work closely with the external safeguarding analysts, reporting back that we have received identification of this incident alongside providing a brief summary of our actions. Entrust Education Technologies also offer further information or support.

9. Students using mobile devices in school

Students who require the use of Laptops or other electronic devices must do so in accordance with the Acceptable User Agreement and with the approval of the Senior IT Technician and parents/carers consent.

10. Students using school devices off site

- All students who are loaned a school device will have to sign an additional agreement and consent form.
- Student/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 as described above.
- 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 who do not have authorised access to the JTFS network
- Students must not share username and password details with anyone else to prevent unauthorised access to the JTFS network

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.

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 Senior 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. How the school will respond to issues of misuse

Where a student 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, described above, 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.

13. 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).

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.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log is stored online. This procedure will be reviewed annually by the DSL. At every review, the procedure will be shared with the governing board.

15. Links with other policies

This Online Safety Procedure is linked to our:

- JTFS Safeguarding Procedure
- Behaviour Procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Comments, Compliments and Complaints procedure
- ICT Security- Acceptable Use Policy
- JT MAT Online Safety Statement