Terrington St Clement Community School

Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, (THIS WILL BE AMENDED TO INCLUDE THE SEPT 2018 VERSION WHICH IS NOT STATUTORY UNTIL 3RD SEPTEMBER) 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 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.

1. Dealing with an Online Safety Incident

The main areas of risk for our school community can be summarised as follows:

Content:

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright and intellectual property

In class:

It is the responsibility of all staff to remind pupils of online safety whenever they use the internet and to make sure children know how to report anything which has upset or worried them.

Pupils will be taught if they see content which has upset of worried them during a lesson they must report it to staff as soon as possible explaining what it is they have seen, on which computer and on which site. If they witness another pupil accessing inappropriate material, they must also report which pupil they witnessed.

If any staff discover a pupil is misusing the internet or abusing internet privileges, the member of staff will primarily explain to the pupil what they are doing wrong and why. They will explain they are at risk of losing internet privileges and take the pupil to discuss their findings with the headteacher (or the deputy headteacher in her absence.) This incident will be recorded as a safeguarding concern and will be recorded in the normal safeguarding folder as a concern.

If this is the first occasion, a warning will be issued to the pupil who will be told they risk losing the privilege of using the internet at break times (for example). If this occurs during a lesson, the pupil will be subject to 1:1 supervision until they have proved they can be trusted.

If the pupil has been warned before, a second record will be made within the safeguarding file, parents will be contacted, close supervision during lessons will be reinstated and break time passes to use the ICT Suite will not be allocated until the teacher and headteacher have agreed it is appropriate to reconsider. If the content viewed is likely to be considered in anyway linked to extremism, this is recorded in the PREVENT file and a referral made if deemed necessary.

Pupil use:

Our Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not. If the school is concerned about a pupil's use of the internet we will take the following steps:

1. Speak first with parents if a pupil is seen to be an under-age user (they may not be aware there is an age limit or their child has created an account and should be given change to make sure the account is deleted).
2. Speak with the child themselves to explain why they are not old enough to use these sites and explain the risks. Show them how to delete their account and how to report concerns. Encourage them to speak with their parents about online safety.
3. If none of the above are successful, seek advice from MASH (the Multi-Agency Safeguarding Hub).
4. If advised to do so, make a referral to MASH. At this point the referral is then taken on by the multi-agency safeguarding tem who decide how to proceed. It may be taken up by the Children's Services Social Care Team or Norfolk Police or bother depending on the concerns and/or the severity of the concern.
5. Report the pupil as an under-age user.

In this school:

• There is strict monitoring and application of the online safety policy, including the ICT Code of Conduct and appropriate range of sanctions.

• Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues

• Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school

• Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible

• The Police will be contacted if one of our staff or pupils receives online communication we consider is particularly disturbing or breaks the law
• We will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA.

Youth Produced Sexual Imagery (Sexting):

Making, possessing or distributing and distributing any imagery of people under 18 which is 'indecent' is illegal. All incidents involving youth produced sexual imagery will be responded to in line with the school's safeguarding policy. When an incident involving youth produced sexual imagery comes to our school's attention we will:

1. Refer the incident to our Designated Safeguarding Lead (DSL) as soon as possible.
2. The DSL will hold an initial review meeting with appropriate school staff
3. There will be subsequent interviews with the young people involved (if appropriate)
4. Parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
5. At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral will be made to children's social care and/or the police immediately.

Staff use:

Any concern about staff misuse which does not follow the ICT Code of Conduct is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors.

2. Education and Curriculum

Pupil online safety curriculum
This school teaches the following content taken from the National Curriculum:
In **Key Stage 1**, pupils will be taught to:

- 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

Pupils 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

and in addition:

• has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience. We use the e-safety progression overview and materials which covers EYFS - Y6 and information is shared with parents.
• will remind students about their responsibilities through the pupil ICT Code of Conduct.

• ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright and intellectual property.

Staff and governor training

This school:

• makes regular up to date training available to staff on online safety issues. This is evidenced through minutes of meetings, certificates and the training log maintained by the school's Admin Assistant.

• provides, as part of the induction process, all staff with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct. This information is also provided in the Staff Expectation Folder which is kept in every classroom.

Parent/Carer awareness and training

This school:

• provides information for parents/carers for online safety on the school website and in Safeguarding Updates which are sent out directly to parents and carers and also uploaded onto the school website.

• provides opportunities to attend event providing online safety advice, guidance and training for parents.

3. ICT Code of Conduct for Staff, Governors and Visitors

All staff, governors and visitors are required to read and agree to the 'Acceptable Use Agreement'. (Appendix 1)

1. All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets.

2. All staff understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.

3. Staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.

4. All staff, Governors and visitors understand they are responsible for all activity carried out under their username.

5. Staff, Governors and visitors will not install any hardware or software on any school owned device without permission from the headteacher who may check with the school's IT provider.

6. All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to the head teacher in line with any disciplinary procedures. This relates to all school-owned devices, including laptops provided by the school.

7. All staff, Governors and visitors will only use the school's email, internet and any related technologies for uses permitted by the Head teacher or Governing Body.

8. All staff, Governors and visitors will ensure all their school generated electronic communications are appropriate and compatible with their role.

9. All staff, Governors and visitors will ensure all data is kept secure by using encryption to secure the data and only sharing this with appropriate bodies in line with GDPR regulations and is used appropriately as authorised by the Head teacher or Governing Body. If in doubt they will seek clarification. This includes taking data off site.

10. Personal devices in the context of school business will not be used unless with explicit permission of the Headteacher.

11. All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

12. All staff, Governors and visitors will only use the approved email system(s) for any school business.

13. Images will only be taken, stored and used for curriculum purposes or for use on the school website. Images will not be distributed outside the school network, including being displayed on the school website without the consent of the subject or of the parent/carer, and the permission of the Head teacher. Parents/carers may request photos to be removed and pupils over the age of 13 may also request historic photos of them to be removed as per the GDPR policy.

14. All staff, Governors and visitors will comply with copyright and intellectual property rights.

15. All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head teacher in line with the school's Safeguarding Policy. If the concern relates to the headteacher's use of technology and/or children's safety, all staff, governors and visitors will report any incidents to the Chair of Governors in line with the school's safeguarding policy.

Staff can expect the Online Safety policy will be communicated to all staff/pupils/community in the following ways:

- Policy is posted on the school website/ staffroom/ classrooms
- Policy is part of school induction pack for new staff, including information and guidance included in the Staff Expectation Folder.
- All staff must read and sign the 'Staff Code of Conduct' annually before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy. This will occur at least annually with updates communicated through weekly Friday meetings.

4. ICT Code of Conduct for Pupils and their parents/carers (Appendix 2)

I will keep myself safe on the internet by:

- only using appropriate websites

- immediately letting a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- always using the school's ICT systems and internet responsibly.
- only using the internet with permission of the adult in class
- not using social networking sites.
- not using chat rooms or agreeing to meet people
- keeping my personal information (including my name, address or telephone number and any passwords) private from anyone other than my teacher or parent/carer
- not following any links without first checking with a trusted adult in school.

5. Email

This school:

- Provides staff with an email account for their professional use (nsix.org.uk) and makes clear personal emails should be through a separate account.
- Three separate e-mail addresses are used for head@, office@ and chairofgovs@
- Will contact the Police if one of our staff or pupils receives an e-mail we consider is particularly disturbing or breaks the law.

Pupils' email:

- We use school provisioned pupil email accounts which can be audited
- Pupils are taught about online safety and the etiquette of using e-mail both in school and at home as part of our online safety curriculum.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff will never use email to transfer staff or pupil personal data unless it is protected with secure encryption.

6. Managing IT and communications systems

School website

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Social networking

- Staff are instructed to always keep professional and private communication separate.
- Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Parents/carers are reminded about social networking age restrictions, risks and protocols through additional communications materials.

Data Security

Management Information System access and data transfer

- The school is registered with the ICO and this registration includes which data we use and how it is used.
- The school is GDPR compliant and uses additional DfE guidance to ensure compliance within the educational setting.

Equipment and Digital Content

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child. This includes named photographs which appear in the local newspaper. Parents/carers have the right to remove their permission at any time in compliance with GDPR policy.
- Staff sign the school's ICT Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment
- Parents are asked to complete a withdrawal of consent form if they do not wish their child to be photographed or video recorded for any purpose. They can amend their consent at any time in writing.

7. Internet access, security and filtering

The school's ICT provider install high level filtering to exclude as many sites as possible. It is then the responsibility of the school to release sites deemed appropriate. This responsibility is devolved to SLT and Phase Leaders only.

8. Reporting concerns about pupils' misuse of the internet:

All staff are registered users of the CPOMS system. Any concerns about pupils' use of the internet will be reported on the CPOMS system by the member of staff discovering the misuse. This automatically alerts the senior designated person for safeguarding and the alternative designated person for safeguarding. Other involved pupils will also be included in the report and all staff who need to be made aware will also be included in the report.

The headteacher will make the decision on whether parents/carers need to be informed. This will depend on the severity of the incident and whether this is the first incident etc. The action taken is also recorded on CPOMS as is every following conversation etc with parents/carers.

August 2018

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I:

- understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets.
- understand it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.
- will not disclose any passwords provided to them by the school or other related authorities.
- understand I responsible for all activity carried out under my username.
- will not install any hardware or software on any school owned device without permission from the headteacher who may check with the school's IT provider.
- understand that permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to the headteacher in line with any disciplinary procedures. This relates to all school-owned devices, including laptops provided by the school.
- will only use the school's email, internet and any related technologies for uses permitted by the Head teacher or Governing Body unless permission is specifically granted from the headteacher.
- will ensure all my school generated electronic communications are appropriate and compatible with my role.
- will ensure all data is kept secure by using encryption to secure data and only share this with appropriate bodies in line with GDPR regulations and use it appropriately as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.
- will not use personal devices in the context of school business unless I have explicit permission of the Headteacher.
- will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory when using school equipment.
- will only use the approved email system(s) for any school business.
- will only take, store and use images for curriculum purposes or for use on the school website. I will not distribute images outside the school network, including displaying them on the school website without the consent of the subject or of the parent/carer, **and** the permission of the Head teacher. If parents/carers request photos to be removed or pupils over the age of 13 request photos to be removed, I will remove these as per the GDPR policy.

14. All staff, Governors and visitors will comply with copyright and intellectual property rights.

15. All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head teacher in line with the school's Safeguarding

Policy. If the concern relates to the headteacher's use of technology and/or children's safety, all staff, governors and visitors will report any incidents to the Chair of Governors in line with the school's safeguarding policy.

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2: Pupils and parents/carers acceptable use agreement.

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
I will keep myself safe on the internet by: • only using appropriate websites • immediately letting a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. • always using the school's ICT systems and internet responsibly. • only using the internet with permission of the adult in class • not using social networking sites. • not using chat rooms or agreeing to meet people • keeping my personal information (including my name, address or telephone number and any passwords) private from anyone other than my teacher or parent/carer • not following any links without first checking with a trusted adult in school	
Signed (pupil):	**Date:**
Parent/carer 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**