# TWEENDYKES SCHOOL

# Online Safety Policy

Date of Policy: Sep 2022
Review Date: Sep 2023

**ETHOS AND VALUES**

Tweendykes School's Online Safety Policy should be read in conjunction with the vision of the school and take into account:

-Tweendykes Child Protection Policy

-ICT Acceptable Use Policy

-Anti-bullying Policy

-Safer working guidance for adults working who work with children and young people in education

-Whistleblowing Policy

All students at Tweendykes School have severe or complex learning difficulties/disabilities (SLD/CLDD) which may affect their ability to communicate. These can include medical needs, specific language impairment, physical and sensory impairment, global developmental delay & autism.

At Tweendykes School we believe that for many of our pupils ICT is fundamental to our curriculum and the lives of our pupils. We want our pupils to access ICT but to do so safely.

We work closely in partnership with local safeguarding arrangements to ensure the safety of our pupils. We complete and monitor a Section 11 and Internet 360 audits termly. An Online Safety Risk assessment is completed annually and is detailed on the school's Safeguarding Calendar.

Termly safeguarding meetings are held in school and online safety is a discussion item.

The online safety policy and any aspects of, are monitored at safeguarding meetings held in school, as well as by **Vicky Cartwright (Online Safety lead), M.Pinchbeck (ICT Governor), Pierre Fenner (designated safeguarding lead) David Percival (deputy safeguarding lead) and Berni Moorcroft (Executive Headteacher).**

**Risks**

People with special educational needs are particularly vulnerable to abuse. The main risks to children are shown in the table below:

| | Commercial | Aggressive | Sexual | Values |
|---|---|---|---|---|
| **Content (child as recipient)** | Adverts<br>Spam<br>Sponsorship<br>Personal Info | Violent/ hateful content<br>Peer on Peer abuse | Pornographic or unwelcome sexual content | Bias<br>Racist<br>Misleading info |
| **Contact (child as participant)** | Tracking<br>Harvesting personal info | Being bullied, harassed or stalked<br>CCE<br>Peer on Peer abuse | Meeting strangers<br>Being groomed<br>CSE | Self-harm<br>Unwelcome persuasions |
| **Conduct (child as actor)** | Illegal downloading<br>Hacking | Bullying or harassing another | Creating and uploading | Providing misleading info/advice |

| | | | | |
|---|---|---|---|---|
| | Gambling<br>Financial scams<br>Terrorism | | inappropriate material | |

**Staffing and online safety**

All teaching and non-teaching staff recognise, are aware of and prioritise online safety issues. High priority is given to online safety cpd. The contribution of the wider school community is valued and integrated.

Online safety cpd requirements are closely monitored and flexible in form to ensure we can respond to national and local issues as they arise. The content of this professional development is dependent on the developmental levels of the pupils staff are working with.

The online safety Coordinator attends regular training events to ensure they are up-to date with any developments. There is at least one whole school cpd yearly, more are arranged if required.

**Access to computing and the internet**

Computers and the Internet have become increasingly accessible for most of our pupils; they access the internet at home and at school through various devices including tablets and phones.

Some pupils may bring mobile phones into school for safety reasons when travelling. All phones must be switched off and put away during the school day.

For most of our pupils, including those with very complex needs, accessing the internet is a favourite activity.

Our pupils will experiment online at home and school, to enable them to take advantage of the many educational and social benefits of new technologies. Our pupils need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users and carers need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviour.

**Pupil emails**

We encourage pupils to use emails to communicate with each other and staff in the school. This must, however, be done safely and within parameters set through liaison between the Online Safety Lead and our external ICT support team.

Pupils' follow an acceptable use contract, which must be signed before pupils are issued with a school email address. This is routinely monitored and reviewed through the school's online safety risk assessment auditing.

**Curriculum**

Computing is a fundamental, integrated part of our school curriculum, as well as a tool to deliver other curriculum areas.

Online safety is covered with pupils depending on their cognitive abilities and complexity of needs.

Whilst the school recognises that online safety is not a specific safeguarding issue, the school recognises that people with special needs are more likely to be victims of online abuse and consequently the school recognises the importance of promoting safety with pupils within the broader context of safeguarding. The school ensures there is a developmental online safety curriculum to help pupils stay safe online.

All pupils access Online Safety teaching through a structured and systematic curriculum (Jigsaw). This is set within a developmental model which also recognises the importance of supporting parents to help keep their children safe when online.

Some pupils will require further, targeted support. This may be through targeted teaching, enhanced staff training to support specific pupils, or through targeted parental support and guidance.

**Access to the internet within the school day and extended onsite school day**

Levels of Internet access are consistent across the school for children and staff separately, and access profiles are to a level appropriate for all members of the organisation.

Our internet filtering is achieved using technology provided by Smoothwall. Staff and pupil activity on devices is monitored through esafe.

Staff wishing to review filtering rules place a request through to the Online safety Coordinator Vicky Cartwright.

A large number of our children struggle to access information through reading, for this reason we made the decision to allow access to YouTube. We are aware that this can lead to greater risks of pupils either deliberately or accidently accessing inappropriate materials. Most pupils now access Youtube, for this reason our pupils for whom it is appropriate have signed an acceptable use agreement. Our pupils are closely monitored while accessing the internet.

**Social Networking**

Social networking sites are blocked at Tweendykes School. Tweendykes currently do not have a Facebook account but do make use of a Twitter account – updates are made through V. Cartwright.

**1. Personal Use of Social Media**

- School staff will not invite, accept or engage in communications with children from the School community in any personal social media whilst in employment at Tweendykes School.

- Any communication received from children on any personal social media sites must be reported following the school reporting procedures (using CPOMS).

- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.

- The school understands that at times it may be appropriate to engage in communications on personal social media with parents (eg parents who are also staff, parents who are 'real' friends outside of work) however staff should always behave in a professional manner, and be mindful of confidentiality issues. Pupils should not be discussed on social media.

- The school should not be named on personal social media accounts, this includes 'place of work' and 'checking in'. Exceptions may include advertising an event etc. If unsure please check with a member of the senior management team.

- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

- All email communication between staff and members of the school community on School business must be made from an official School email account (Outlook or Outlook 365).

- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.

- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts. School life should be celebrated and not commented on in a negative manner.

- Staff should not accept any current student of any age or any ex-student of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account. The school advises staff to not accept any former students over the age of 18.

**2. School Social Media account**

There are many legitimate uses of social media within the curriculum and to support student learning. There are also many possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official School email account.

- The URL and identity of the site should be notified to the appropriate Head of Faculty or member of SLT before access is permitted for students.

- The content of any School sanctioned social media site should be solely professional and should reflect well on the School.

- Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on School social media accounts.

- Care must be taken that any links to external sites from the account are appropriate and safe.

- Any inappropriate comments on or abuse of School sanctioned social media should immediately be removed and reported to a Safeguarding Officer for further investigation.

- Staff should not engage with any direct messaging of students through social media where the message is not public.

- All social media accounts created for educational purposes should include a link to the ICT & Acceptable Use Policy on the School website. This will indicate that the account is officially sanctioned by Tweendykes School.

**Cyber bullying**

Cyber bullying (along with all forms of bullying) is not tolerated at Tweendykes School, procedures for dealing with all forms of bullying are laid down in our anti-bullying policy.

Dealing with cyber bullying is a curriculum area to be covered with our pupils.

Sanctions for those involved in cyber bullying will include:

*Internet access may be suspended for the user for a period of time.

*Parents/Carers will be informed.

Peer on Peer abuse can take place online in the form of Cyberbullying, Domestic Abuse, CSE, Harmful Sexual Behaviour, Sexual Harassment.

Please refer to the HET Safeguarding Policy for further definition.

**CyberBullying**

This may be defined as any deliberately hurtful behaviour, usually but not exclusively repeated over a period of time, which intentionally hurts another pupil or group physically or emotionally. It is often difficult for those being bullied to defend themselves, and it is often motivated by prejudice.

Cyber-bullying, which is defined as the use of ICT by an individual or group in a way that is intended to upset others. Examples include using social websites, mobile phones, text messaging, photographs, video and e-mail.

## Sexual abuse

Pupils at Tweendykes are active online and as such are equally vulnerable online as well as offline. All staff working with children must maintain an attitude of 'it could happen here' and remain mindful that sexual harassment and/or sexual violence could be happening even where it is not being reported.

Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face to face (both physically and verbally) and are never acceptable.

**Images of pupils**

Images taken of pupils should be on school owned devices only, personal mobile phones should not be used. If for any reason a mobile phone is used to 'not miss an important event' this much be taken off as soon as possible and Vicky Cartwright informed.

Parental Permission slips to use images of pupils are signed yearly. Those pupils without permission, are made known to the relevant staff. Parents are asked not to take images of pupils at events.

**Parents**

The school recognises that within the context of a developmental Online Safety curriculum parents are key partners in ensuring that pupils are able to stay safe when online. The school is committed to making sure parents are aware and have the skills necessary to help keep their children safe online at home.

The school provides support and guidance on its website, through routine communications with parents and through regular in-school events.

Parents are informed they can contact us directly with any concerns or support requirements they may have.

**Reporting Incidents**

If an incident occurs where staff are concerned for the safety of the child, the reporting procedure as laid down in the child protection policy is to be followed. A CPOMS entry using the 'Online Safety' button is completed. This is sent directly to the Designated Safeguarding Lead and to the Online Safety Lead.

**Further Information, help and guidance**

Further guidance is available to staff on the team site under the 'Curriculum' page.

Further information can be found in the statutory guidance *'Keeping children safe in education'*

Various documents and advice are available on the internet. Childnet (http://www.childnet.com/) is very good.

The following people are available in school:-

**M.Pinchbeck (ICT Governor), Pierre Fenner (Headteacher), David Percival (Designated Safeguarding Lead)**

**Policy Review**

A review of the policy will be undertaken in line with the policy review timetable and any amendments or updates will be reported to the Governing Body.

Any new legislation or directives will be incorporated into the policy as necessary