E-Safety Policy 2025

Amended on: 22 Jan 2025

Review Date: September 2025 or sooner in the event of an issue arising
Our E–Safety Policy has been written by Do Talk Write (DTW), building on the national guidance.
This policy relates to best practice as promoted by CEOP, the government's national child protection agency for E-Safety.

DTW's Director takes responsibility for E-Safety.

Do Talk Write E-Safety Policy

Overall vision for E-Safety

Keeping students safe is of the highest priority. Our E-Safety vision is simple.

Safe to learn

We want our young people to work thoughtfully in a safe environment whilst in our care and whilst away from our care.

Safe for life

We want young people to live a safe digital life, harnessing the great opportunities which technology brings us whilst feeling empowered to make good choices to stay safe with technology.

What do we mean by technology?

Technology within this policy means electronic equipment which provides us with information. Technology is another word for ICT (Information Communication Technology). This includes the hardware, such as mobile phones, laptops, tablets, iPads, desktop computers and software which are the programmes and applications which people use. Examples of software programmes include Microsoft Office tools such as Word. This definition also includes the things which are harder to see, such as the internet and computer network. These are types of ICT services. Throughout the policy we may use the term technology and ICT interchangeably.

How does technology benefit education at DTW?

ICT benefits learning and teaching in the following ways:

- Provides an engaging and motivational way to learn, especially for some of our most disengaged learners.
- Allows learners access to a rich variety of multimodal information e.g. video, audio, images, text, to engage numerous learning styles and preferences.
- Allows learners to connect to learning in accessible ways e.g. by providing a writing framework or having the computer read instructions to them to support various learning needs.
- Supports high quality teaching through diverse and interactive resources.
- Supports a collaborative approach to learning in a managed, structured, and controlled way as a scaffold towards face-to-face collaboration, our final goal.
- Supports personalisation by providing flexibility in the pace, place and time of learning.
- Culturally enriching by connecting learners to people and communities in different localities, opening minds and raising awareness of our cultural heritage and responsibility as global citizens.

The internet at DTW can provide the following specific benefits:

- Access to worldwide educational resources.
- Educational and cultural exchanges between learners worldwide.
- Access to experts in many fields for learners and staff.
- Professional development for staff through access to national developments, educational materials, and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data through our online learning platform.
- Access to learning wherever and whenever convenient.
- Communication systems with up-to-date information.

How can internet use enhance learning?

- Internet research, including the skills of knowledge location, retrieval, and evaluation.
- Online activities that support the learning outcomes.
- Learners can use web-based tools to collaborate on learning activities.

Learners will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Copyright law will be adhered to by DTW when using materials from the Internet.

Induction

When learners are inducted at DTW, parents/carers and learners are asked to sign a DTW Learner Consent Form. It also sets out in the agreement that parents and learners give us permission to use and store learner information at DTW as outlined in GDPR. Completion of this agreement is a prerequisite of joining DTW. This agreement needs to be signed and a copy retained by the parent/career and another to be retained by DTW.

Managing Information

- Staff have access to email and DTW OneDrive and are advised of their responsibility during induction.
- Updating virus protection regularly on all DTW issued and personal ICT equipment used for work by employees.
- Users are required to use two-step authentication to ensure access to data is secured to the highest possible levels. Safeguarding information is only shared via CPOMS by staff.
- Personal data should only be shared and stored as per the GDPR policy.
- E-Safety training is undertaken by all staff and is updated yearly.
- Guidance available on website. Online safety (e-safety) and schools | NSPCC Learning or Teachers & professionals | Childnet

Social Media

At induction, all staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally or personally. They should be made aware of the importance of considering

the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status at DTW.

In different industries, there are varying expectations around the use of social media e.g. Facebook, Twitter and LinkedIn. As DTW is an educational provider we set very high standards around the responsible use of social media.

All staff have a responsibility to ensure their actions when using social media do not compromise the integrity and professional standing of themselves and DTW. This applies to social media use in work time and outside of work time.

As internet sites and resources are increasingly adding a social element to their appearance and operation, staff should consider all web resources carefully and ensure they are appropriate and safe for use.

Learner use of social media

- Where filtering is in operation, access to social media and social networking sites can be controlled by filtering software. Staff are to monitor learners whilst using public and issued DTW ICT equipment.
- Learners will be advised on security and privacy online. Concerns regarding learners' use of social networking, social media, and personal publishing sites will be raised with their parents/carers, particularly when concerning learners' underage use of sites.
- Learners will be advised never to give out personal details of any kind which may identify them and/or their location (as agreed at induction).
- Further parent advice can be sought from Parent Zone | At the heart of digital family life

Staff use of social media

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction including safe and professional behaviour.
- DTW reserves the right to follow the Safer Recruitment Policy when an individual applies to be DTW member of staff and will complete online/Social Media checks of all applicants.
- Staff should not use social media to 'sound off' about their day or about staff and/or learners.
- Staff should not use social media to anonymised teaching and learning experiences, however discussing resources and strategies would be considered acceptable.
- Staff should not relate any discussions to DTW or allow a learner to be identified in any way.
- Staff should refuse any contact from learners or parents through social media. This includes ex-learners and ex-parents.
- A good rule of thumb is to consider; How would a director/my employer feel if this message/post was read by them?

An excellent guide for staff who use social media in both professional and personal life should be read: Childnet — Online safety for young people

Keeping Children Safe in Education (KCSIE)

Keeping children safe in education - GOV.UK (www.gov.uk)

An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring is included in safeguarding and child protection training at induction for all staff.

Use of social media for communications within DTW

At DTW we use social media to support communication and marketing activities.

- We adhere to the following: Restricting access to social media accounts only to authorised staff.
- We don't use social media to make political points or raise controversial issues.
- We respond to any criticism in a timely and positive fashion with the outcome demonstrating our openness, transparency, and desire to work in a positive and proactive way with families and organisations.
- We regularly review our communications to ensure we act and communicate appropriately for the social media tool - in line with our corporate image and responsibility.

Keeping social media communications positive and productive.

- We restrict access to official DTW social media accounts only to authorised staff, including the parent coordinator.
- The group is monitored by our director.
- All posted messages must adhere to our rules of use.
- We reserve the right to remove users who break the rules of use.

How will filtering be managed?

- Where a learner accesses a learning location (e.g. a library) with computers with filtered internet, it is the staff's responsibility to ensure E-Safety is adhered to. The learner should not be left unattended whilst using the ICT equipment/the internet.
- Activities should be thoughtfully planned to make sure that only specific, relevant sites are accessed.
- Staff are responsible for their own devices and should not allow a learner access to them. They should ensure that their devices have adequate protection and are password protected. Staff should ensure that, when not used, their devices are closed and are not left unattended.
- DTW Issued ICT (Laptops) are issued for the use of Learners only (with support from the tutor). Tutors are to monitor the learner at all times whilst using the ICT. DTW Staff are not to use the DTW Issued laptops for work or personal use. Each learner must access their own profile whilst using the device and must be connected to the internet to ensure they are filtered and monitored correctly.

How are emerging technologies managed?

- Emerging technology means any new ICT hardware or software innovations.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use at DTW is allowed. All DTW devices are filtered appropriately for our learners and are remotely monitored by the DSL via the SENSO system.
- Learners will be instructed about safe and appropriate use of personal devices during DTW sessions.

How should personal data be protected?

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998 and GDPR.
- All staff undergo GDPR training via SSS.
- DTW will comply with freedom of information requests in accordance with the Freedom of Information Act 2000 and recommendations from the Information Commissioner's Office.
- DTW demonstrates this compliance by registering with the Information Commissioner's Office.

How will risks be assessed?

- DTW will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via ICT. DTW cannot accept liability for the material accessed, or any consequences resulting from internet use on non DTW devices.
- DTW staff will meet regularly to ensure it is adequate and being implemented appropriately. They will identify, assess, and ensure methods are in place to minimise risks.

How will DTW respond to any incidents of concern?

- All members of staff will be informed about the procedure for reporting E-Safety to the relevant Learning Managers, DSL, and Director. Concerns (such as breaches of filtering, cyberbullying, illegal content etc.) must be reported immediately.
- The DSL will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately as per KCSIE.
- Safeguarding breaches are monitored remotely via the SENSO alert system and inform the DSL immediately of any concerns. The DSL will then take appropriate action.
- DTW will inform parents/carers of any incidents of concern as and when required. In most cases, this will be in person on the day of the incident.
- After any investigations are completed, DTW will debrief, identify lessons learnt and implement any changes required and if necessary, contact CEOP.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of DTW or learner will not be tolerated.
- All incidents of cyberbullying reported via CPOMS to the Learning Managers, DSL and Director who will investigate and inform parents of outcomes. The Police will be contacted if a criminal offence is suspected.

Sanctions for those involved in cyberbullying may include:

- Making a copy of the material as evidence.
- Those involved will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the person involved refuses or is unable to delete content.

- Internet access may be suspended at DTW for the user for a period of time. Other sanctions for all involved may also be used in accordance with other policies at DTW.
- Parent/carers of learners involved will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will mobile phones and mobile devices be managed?

The use of home-owned mobile phones, tablets, iPods etc. and other personal devices by learners and staff is prohibited at DTW. Only DTW issued ICT (or a public Library computer) can be used with a Learner during a DTW session. DTW Staff are not to share their personal mobile number with a Learner. Tutors should not communicate with Learners directly via mobile phone (Calls/text or WhatsApp groups etc) and must ensure all of this Commnication is via a parent/guardian. This includes Learners who are also adults.

Staff Use of Personal Devices:

- Home-owned devices (laptops, tablets, iPods, mobile phones etc.) can only be used by the tutor.
- Personal mobile phones are the sole responsibility of the tutor.
- Electronic devices of all kinds that are brought into lessons are the responsibility of the user. DTW accepts no responsibility for the loss, theft or damage of such items or responsibility for any adverse health effects caused by any such devices, either potential or actual.
- If staff need to take photographs and/or videos for work evidence, for example written work or an art project, (the image must not contain the child) any images or video created at DTW on a home-owned device must be deleted from the device once used for the specific purpose. Staff are discouraged to include the learner or any child in any photographs taken (including in the background) and if essential for learning evidence (is a requirement for a recognised qualification), written consent from parent/carers must be sought prior to any image of a child is taken, including the reason why and what is the purpose of the photograph/video. Only DTW devices may be used to take photographs/videos of our learners as evidence of work and once uploaded for the evidence purpose must be deleted immediately. Staff must not take photographs/videos of Learners on their personally owned mobile phones/devices.
- Care should be taken when using a mobile phone or device in school time so as not to compromise professional expectations; think about who can view or hear the content from a mobile device? Think about how a director would react to viewing this content and could your professional integrity be negatively impacted?
- If a member of staff breaches the policy, then disciplinary action may be taken.
- Staff are not allowed to contact parent/carers or learners once the learner has left DTW.
- All DTW issued ICT must be returned to DTW if the staff member ceases to work for DTW. Failure to do so will result in a fine of the cost of the equipment.
- Faults with DTW ICT equipment must be reported immediately to Bubble IT and the Learning Manager.
- Any Loss, damage (whether intentional or not) or misuse of DTW ICT equipment must be reported to a Learning Manager immediately.

Learners Use of Personal Devices:

- We recognise that for many learners they are reliant on access to a mobile phone. Rather than a blanket policy covering all key stages and situations, we expect that appropriate use of mobile phones is encouraged and monitored by all staff.
- At DTW, if a learner needs to contact his/her parents/carers, the tutor will facilitate this. Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the relevant Learning Manager or the director of DTW.
- Electronic devices of all kinds that are brought into lessons are the responsibility of the user. DTW accepts no responsibility for the loss, theft or damage of such items or responsibility for any adverse health effects caused by any such devices, either potential or actual.
- Where the use of a mobile device affects engagement in learning, appropriate responses should be taken. Advice should be sought by contacting the relevant Learning Manager.

Communication between DTW Staff and DTW Learner via email

- DTW Staff are able to send/ receive work for the Learner via their DTW email address/learner DTW email address. This correspondence will be filtered and monitored via the SENSO system when accessed via a DTW laptop by the learner. Staff are reminded to ensure that this correspondence is to be kept to a minimum, only responded to during normal working hours and is professional at all times. Staff are encouraged to copy in another member of DTW staff, Learning manager or parent/guardian when sending emails to learners about their work. Any concerns or out of hours contact is to be reported to the DSL or Learning Manager.

How will the E-Safety policy be discussed with staff?

- The E-Safety Policy will be formally provided and discussed with all members of staff at induction.
- E-Safety training will be provided to all staff via SSS.
- All staff members will be made aware that their online conduct outside of school could impact on their role and reputation within the school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- E-Safety updates will be shared with parents/carers by the DSL to share best practice and resources.

Review

This policy will be reviewed annually as the nature of E-Safety is rapidly changing. Please remember that this is not a “straight jacket” to adhere rigorously to, these guidelines will help to prompt and inform your unique response. All E-Safety responses should be coordinated with the director, DSL, and the relevant Learning Manager.

An inappropriate website is accessed unintentionally by a Learner or member of staff.

- Play the situation down; don’t make it into a drama. Ask the learner to turn off the monitor, minimise the web page or close the laptop lid, so the image or text cannot be seen by others. Make a note of the web address in the URL bar.

- Discreetly discuss why the site is inappropriate with the Learner, or any issues that their experience might raise. Tell them who else they could talk to if what they have seen worries them e.g. parent/carer, CEOP.
- Report to the Director/Learning Manager/DSL as soon after the event as is reasonably possible and follow up with a CPOMS entry. The DSL/Learning Manager decides whether it is appropriate to inform parents/carers of any additional young people who viewed the site. Details to be reported to Bubble IT to ensure this is restricted immediately.

An inappropriate website is accessed intentionally by a learner.

- Explain why they should not be viewing this content. Show them where to find the appropriate and relevant information they are searching for.
- Preserve any evidence through print outs or screen capture.
- Inform parents/carers, if necessary, as this may be a pattern of negative behaviour which goes unchecked at home.
- Contact the Learning Manger and/or the DSL and record the incident as an E-Safety concern via CPOMS. Details to be reported to Bubble IT to ensure this is restricted immediately.

You and a learner observe another adult using ICT equipment inappropriately on a shared premises (e.g. at a Library viewing videos on YouTube which are clearly unsuitable.)

- Report the misuse immediately to the venue manager and then the DSL. Do not challenge the person who you observed.
  In an extreme case where the Director deems the material is of an illegal nature:
- Contact the Police or CEOP and follow their advice.
- Record incident as an E-Safety concern on CPOMS.

Malicious or threatening comments are posted on an Internet site about a learner or member of staff.

- Secure and preserve any evidence using screen capture or photographing a monitor or mobile phone.
- Inform the Learning Manager/DSL/Director via CPOMS who will work with the member of staff to preserve the evidence and identify the comments, which are upsetting for the member of staff or learner. Discuss with parents/carers concerned. Report to the Police if necessary.
- Inform and request the comments be removed if the site is administered externally.
- Send all the evidence to CEOP at www.ceop.gov.uk, take guidance over the nature of the comments.
- Endeavour to trace the origin and inform police if appropriate.
- Contact the Learning Manger and/or the DSL and record the incident as an E-Safety concern via CPOMS.

You are concerned that a learner's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the Learner.

- Report to and discuss with the Learning Manager and DSL as soon as possible. Parents/carers will be contacted immediately.

- In partnership with parents/carers, advise the Learner on how to terminate the communication and save all evidence offering confidential support to do so if needed.
- Consider taking action to report/suspend the account ensuring evidence is retained, do not delete the social network account at this stage. Offer advice and direct support to parent re. setting up safe internet etc...
- Contact CEOP www.ceop.gov.uk with parent/carer and Learner and ask for advice.
- With the Director/Learning Manager/DSL and advice from CEOP, consider the involvement of other professionals.
- Take steps to check actions have been successful in stopping inappropriate contact.
- Record the incident as an E-Safety concern via CPOMS

A member of staff overhears a conversation between two learners. The conversation was meant to be private. One of the learners mentions that she is meeting up with a girl tonight, who she met through a Facebook/social network group.

- Consider that the learner may be at risk of meeting an **adult** stranger tonight, without parental knowledge who is masquerading as a young person.
- Inform the Director/Learning Manager/DSL and plan a response before the end of the school day on the day of the incident. The DSL/ Learning Manager may decide that it is necessary to supervise the Learner until a parent/carer can be contacted.
- Contact home to ascertain whether the parents/carers are accompanying the learner to meet their "online" friend.
- Check if the parent is aware of what social media their child is accessing.
- Contact the Learning Manger and/or the DSL and record the incident via CPOMS.

A current or ex-learner asks you to be their online friend on a social network such as Facebook.

- Politely decline the learner's offer and explain the inappropriateness of the request.
- The same should also apply for online gaming, text messaging and any other forms of communication.
- If the learner (ex-learner) persists in contacting you, i.e. after you have declined to connect/befriend them, contact the Learning Manager and/or the DSL and record the incident as an E-Safety concern via CPOMS.

Significant Incident form to be completed.

Where there is immediate danger to a learner

Contact the DSL immediately by phone. If you are unable to contact the Safeguarding lead, contact a Learning Manager who is also a trained D-DSL. Stress that this is a child protection issue, and it is imperative that a message is received by a Safeguarding lead immediately, to make contact.

Useful e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): CEOP Safety Centre

Childline: Childline | Childline

Childnet: Childnet — Online safety for young people

Think U Know website : CEOP Education (thinkuknow.co.uk)

360 safe – e-safety self-review tool: Online Safety Self-Review Tool for Schools | 360safe

Keeping Children Safe in Education 2023 Keeping children safe in education - GOV.UK (www.gov.uk)

KS2

Knowledge and understanding	Skills and responsibilities	Suggested activities
Rules help keep children safe when exchanging learning and ideas online.	Identify the risks and rewards of using the internet at home and school.	Use the internet to research and gather information.

Understand that websites may not be accurate or reliable and can be persuasive or biased. Begin to understand that the internet contains facts and opinions. Understand the need to keep passwords safe and the importance of strong passwords. Understand that information shared using ICT can be easily copied and made public.	Know and put into practice basic E-Safety rules and healthy choices e.g. limiting screen time. Begin to understand the difference between copying and pasting from the internet and re-wording information in your own words. Consider when to open an email or attachment. Understand why we use an avatar or alias online. Respect others ICT work and messages. Understand that unkind messages and pictures will upset others and may constitute bullying.	Think about when we use the internet and who can help us to stay safe. Share and exchange ideas using ICT with others beyond the school e.g. emailing a charity or partner school as a whole class under adult supervision. Design nicknames and avatars, begin to create a class Social Media page offline e.g. so positive attitudes towards sharing information can begin to be established. Share information between children safely e.g. emailing within the class.

KS3

Knowledge and understanding	Skills and responsibilities	Suggested activities

Explore and discuss positive and negative impacts of ICT use at home and school. Understand the E-Safety rules in school and broader rules e.g. Age ratings on games, minimum age limit of social media.	Make good choices when using ICT, with reference to the E-Safety rules. Know where to find out about E-Safety e.g. use of the CEOP website. Know how to stay safe on social media sites.	Know the consequences of sharing information online: Use CEOP video Jigsaw. Discuss the eternal nature of content posted online and the lack of control a user has. Quote sources and respect copyright when using ICT.

Understand what personal information is and why it is risky to share this with people you do not know. Understand the need to evaluate content on the internet carefully and establish reasons why people may put inaccurate information on the internet. Begin to explore internet scams such as phishing and spam and know how to respond to such threats. Understand copyright and how to use information from the internet in a legal and respectful way.	Create and use strong passwords. Evaluate websites and the content on them, identifying any risks and how to manage these. Know they have a right to be protected from inappropriate use of ICT and a responsibility to others to respect their rights e.g. when using a digital camera, requesting consent from the subject.	Consider which communication tools are most appropriate for the content, speed, audience etc. Use spoof websites such as Northwest Pacific Octopus to evaluate information on the web and discuss fact/opinion and plausibility. Use cross referencing (other websites and books) to ascertain facts.