

# Down Syndrome Development Trust

## Online safety policy (2020)

DSDT believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

The purpose of DSDT's online safety policy is to:

1. Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that DSDT's systems of usage is a safe and secure environment.
2. Safeguard and protect all members of the DSDT community online.
3. Raise awareness with all members of the DSDT community regarding the potential risks as well as benefits of technology.
4. To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
5. Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

### To whom this policy applies

- This policy applies to all staff including the Trustee's, management teams, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the DSDT (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with DSDT issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be used in conjunction with other relevant DSDT policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).
- The DSDT will ensure that all images are used in accordance with our image use policy with written permission from parents or carers will always be obtained before images/videos of participants are electronically published.
- All members of staff are provided with a specific DSDT email address to use for any official communication.
- The use of personal email addresses by staff for any official charity business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the DSDT community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the DSDT online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.

### Videoconferencing

- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Videoconferencing contact information will not be put on the DSDT's website.
- The equipment will be kept securely and if necessary locked away when not in use.

- DSDT videoconferencing equipment will not be used without permission.
- Responsibility for the use of the videoconferencing equipment outside of designated session times will be established with care.
- Staff will ensure that external videoconferences are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Users
- Video conferencing will be supervised appropriately for the participant's age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.
- There will be two members of staff monitoring every event.
- Parents will be required to be present in the room at all times.
- Expectations regarding safe and responsible use of social media will apply to all members of DSDT's community and exist in order to safeguard all involved, on and offline.
- Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of DSDT's community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of DSDT's community.
- All members of DSDT's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The DSDT will control participants and staff access to social media and social networking sites whilst taking part in sessions.
- Inappropriate use of social media may result in disciplinary or legal action.
- Any concerns regarding the online conduct of any member of DSDT community on social media sites should be reported to the DSDT Trustee's team and will be managed in accordance with existing policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of DSDT's policy may result in criminal, disciplinary or civil action being taken, and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with the relevant DSDT policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

## Official use of social media

- Official use of social media sites by DSDT will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the DSDT.
- Official DSDT social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use DSDT provided email addresses to register for and manage official DSDT approved social media channels.
- Members of staff running official DSDT social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official DSDT social media platforms will be clear, transparent and open to scrutiny.

- Any online publication on official charity social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the DSDT will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official DSDT social media sites/channels in accordance with the DSDT image use policy.
- Information about safe and responsible use of DSDT's social media channels will be communicated clearly and regularly to all participants.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the DSDT website and take place with approval from the Trustee's and management team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and participants will be informed of any official DSDT social media use, along with expectations for safe use and DSDT action taken to safeguard the community.
- Public communications on behalf of the DSDT will, where possible, be read and agreed by at least one other colleague.
- The DSDT social media account will link back to the DSDT website and/or Acceptable Use Policy to demonstrate that the account is official.
- The DSDT will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

## Staff official use of social media

- Relevant for all settings
- If members of staff are participating in online activity as part of their capacity as an employee of the DSDT, then they are requested to be professional at all times and that they are an ambassador for the charity.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the DSDT.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the DSDT, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the DSDT social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the DSDT unless they are authorised to do so.
- Staff using social media officially will inform their line manager, of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with participants.

## Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the DSDT Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past participants or current or past participants' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/member of Leadership Team/headteacher.

- All communication between staff and members of the DSDT community on charity business will take place via official approved communication channels (such as DSDT email address or phone numbers). Staff must not use personal accounts or information to make contact with participants or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the management.
- Any communication from participants/parents received on personal social media accounts will be reported to the designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about participants and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with DSDT policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the DSDT.
- Member of staff will ensure that they do not represent their personal views as that on DSDT social media.
- DSDT email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the DSDT's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

## Children's use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the DSDT's Acceptable Use Policy.
- Personal publishing on social media sites will be taught to children as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Children will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Children will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Children will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Children will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with participants and written parental consent will be obtained, as required.
- Any official social media activity involving participants will be moderated by the DSDT where possible.
- The DSDT is aware that many popular social media sites state that they are not for children under the age of 13, therefore the DSDT will not create accounts within our setting specifically for children under this age.
- Any concerns regarding participants' use of social networking, social media and personal publishing sites, both at home and at DSDT activities, will be dealt with in accordance with existing DSDT's policies including

anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

- DSDT is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the management team will ensure that appropriate risk assessments are carried out before use in the DSDT is allowed.
- The DSDT will ensure that appropriate filtering systems are in place to prevent staff and participants from accessing unsuitable or illegal content.
- The DSDT 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 a DSDT computer or device.
- The DSDT will audit technology use to establish if the online safety (e-Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the management team.
- Filtering decisions, internet access and device use by participants and staff will be reviewed regularly by the management team.
- The DSDT will maintain a current record of all staff and participants who are granted access to electronic communications.
- All staff, participants and visitors will read the DSDT Acceptable Use Policy before using any DSDT's ICT resources.
- Parents will be informed that participants will be provided with supervised Internet access which is appropriate to their age and ability.
- When considering access for vulnerable members of the charity's community (such as with children with special education needs) the DSDT will make decisions based on the specific needs and understanding of the children.
- The DSDT is aware that some children may be considered to be more vulnerable than most children online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety).

## Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of the DSDT safeguarding practice.
- To protect all staff and participants, the DSDT will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Management Team and will have clear procedures for reporting issues or concerns.
- The DSDT will highlight useful online tools which staff should use with children. These tools will vary according to the age and ability of the participants.
- All members of staff will be made aware that their online conduct out of work could have an impact on their role and reputation within the DSDT. 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.

## Engagement and education of parents and carers

- DSDT recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- A partnership approach to online safety at home and with parents will be encouraged. This may include offering demonstrations and suggestions for safe home Internet use or highlighting online safety.

- Parents will be encouraged to role model positive behaviour for their children online. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The Management team will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded and will ensure that online safety concerns are escalated and reported to relevant agencies in line with the appropriate Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the DSDT complaints procedure.
- Children, parents and staff will be informed of the DSDT complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the DSDT community will need to be aware of the importance of confidentiality and the need to follow the official DSDT procedures for reporting concerns.
- All members of the DSDT community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the DSDT community.
- The DSDT will manage online safety (e-Safety) incidents in accordance with the DSDT discipline/behaviour policy where appropriate
- The DSDT management will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the DSDT will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the DSDT will contact the local Safeguards Team or Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- If the DSDT is unsure how to proceed with any incidents of concern, then the incident will be escalated to the LA Safeguarding Team.
- Parents and children will need to work in partnership with the DSDT to resolve issues.

End