Online Safety Policy and SOP

Mandatory Read for school staff

Lead Director Samantha Newton	**Date Reviewed** **May 2022**
Lead Author(s) Launa Randles	**Date Drafted** May 2022
Recommended By Educational Governance Committee	**Endorsed Date** [MONTH YYYY]
Approved By Educational Governance Committee	**Ratified Date** NOV 2022
Published Date DEC 2022	**Next Review Date** DEC 2024

Contents

The policy file name should be in the format [XYZ Policy] + [v] + [version number]. The following version numbering system should be used:

Initial drafting	0.1
First final, issued version	
Draft amendments to version 1.0	
Second final, issued version	
Draft amendments to version 2.0	

Policy

1 Purpose and Objectives

The Children's Trust School is a non-maintained special school supporting children aged 2-19 with complex Education Health Therapy and Care (EHTC) needs resulting in multiple barriers to learning. Primary needs include all children having complex health including palliative and degenerative conditions, communication and interaction, cognition and learning, physical and sensory, social and emotional needs. For all the children daily use of electronic devices positively impacts their education. It provides communication, participation and active engagement.

As a school we need to ensure the children are safe in their learning. We understand the need of age-respectful, meaningful, and accessible technology and the essential need to safeguard from potentially harmful and inappropriate online material.

With an effective approach to online safety, we ensure the staff monitor safe use of all devices and understand how to identify, intervene in, and escalate any concerns. We recognise the adults around the child and their behaviours are key and they **must** take an active role in creating/maintaining the safe learning environment

Our intention is to ensure that all children (supported by the adults) have daily access to essential devices, they will be responsible users and stay safe whilst using internet and other adapted technologies supporting educational & personal use, on the school site, at home on a school residential house.

Our approach to online safety does address the 4 categories of risk as outlined in KCSIE:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Details of the process specific to the children and young people at The Children's Trust School appears in the Standard Operating Procedure (SOP).

2 Scope

This policy applies to:

- All Children/young people, family, staff and Volunteers at The Children's Trust School
- All contractors and visitors to The Children's Trust School / all systems / all data processing activities

3. Definition

Unless otherwise stated, the words or expressions contained in this document shall have the following meaning:

TCTS	The Children's Trust School
SOP	Standard Operating Procedure
IRAR	Incident & Risk Assessment reporting
IMPACTS	School curriculum
Promises	Our organisational cultures & values; Child first / Aim High / Care Deeply / Be open / Own it
KCSIE	Keeping Children Safe in Education
DSL	Designated Safeguard Lead
DDSL	Deputy Designated Safeguard Lead
LAC	Looked After Child
IRAR	Incident & Risk Assessment Reporting
Regulated area	Regulated areas are where care and education is delivered to the children
Personal Electronic Device	Mobile / SMART
ECT	Environmental Control Technology
Cyber-bullying	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.
IGC	Information Governance Committee

4. Policy statement

Policy 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.
Online safety awareness is for the children, parents, staff including volunteers and governors.

Our pupils, due to their need, are more vulnerable and do rely on the frequent use of technology devices to engage with the curriculum, their world, and people around them. Policy ensures safety of children and young people at The Children's Trust who need adult support to recognise and avoid online safety risks. Ultimately, all systems operate with the best interests of the child.

Our staff and volunteers are fully trained with our approach to online safety and learning. Staff can raise, intervene, escalate all concerns. Staff know the children and advocate for new specialist technology to ensure we continually meet the access needs of our pupils. All staff maintain the attitude 'it could happen here'

Our parents are informed & given advice on their child's personal device/s, to facilitate safe and meaningful use. The best & safe virtual learning practice is unique to the learner and requires adult presence.

As a school in a wider organisation, we operate in line with our promises and within the law in terms of how we use online devices.

5 Stakeholder Consultation

Appendix 1 details the stakeholders who were consulted in the development of this policy and have done a critical read.

6. Related Policies

This online safety policy is linked to our:

- Child protection and safeguarding
- Use of electronic communication devices
- Incident Reporting and Investigation including Duty of Candour
- Behaviour of Concern
- Staff disciplinary
- Low Level Concern
- Staff Code of Conduct (school and within TCT staff handbook 2021)
- Data protection
- Complaints procedure
- ICT acceptable use
- Relationship and sex education (RSE)
- Home Learning Policy

7. External References and Guidance

- Keeping Children Safe in Education
- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- 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.

3 Roles and responsibilities

1.1 The School governors

The school governors have overall responsibility for monitoring this policy and holding the head of school to account for its implementation.

The nominated governor will regularly meet with appropriate staff to discuss online safety, monitor online safety incidents & subsequent learning (located on IRAR)

The governor who oversees online safety is Viv Berkeley.

All governors will:

- Ensure that they have read and understand this policy
- Ensure they have read and understood KCSIE (all parts and appendices with reference to the management safeguarding part 2)
- Provide evidence of completing annual PREVENT training
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and children and young people with SEND. Recognise the importance a 'one size fits all' approach is not appropriate for all children in all situations, and a more personalised or contextualised approach is required.

1.2 The Head of School / Director of Education

The Head of School / Director of Education is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

1.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies' roles and responsibilities are set out in KCSIE (Appendix C) and TCT child protection and safeguarding policy

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

- Working with school management & The Children's Trust Head of IT & Transformation and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school safeguarding children & young people policy
- Ensuring that any online safety incidents are logged on the IRAR electronic system and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are logged on the IRAR electronic system and dealt with appropriately
- Delivering staff training and providing 'learning' from incidents
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety to the governors via Educational Governance Committee reports and monitoring governors' visits
- The DDSL for LAC to work with local authorities to promote educational achievement using the safe online resources & technology devices
- With IT managers monitor risk & undertake IT provision audits (online 360)
- Raise online safety awareness (school participate in national online awareness day / training / supervision)
- Update (annually) the school code of conduct to include staff appropriate use of all online devices.

The Lead DSL is Launa Randles

The DDSL supporting online safety is Elaine Lush

The DDSL with oversight of purchase & impact of pupil premium is Maz Hanlon

1.5 The Head of IT & Transformation

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children and young people are kept 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
- Protecting students' data on TCT Networks and devices, as a means to prevent future exploitation.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- To review categories blocked by the Firewall with the IGC, Chaired by the Director of Education to Ensure 'over blocking' does not lead to unreasonable restrictions
- To be 'on the who needs to know' list of all online safety incidents / cyber bullying in order to increase safeguarding measures & reduce risk

The Head of IT & Transformation Richard Groom

1.6 Assistive Technology Team

- Ensure that the children and young people have access to the assistive technology that enables them to access classroom activities
- Provide training and ongoing support to ensure the team around the child have the skills required to implement the assistive technology in an effective manner
- Rapidly support and correct assistive technology failures and configurations that would prevent the child or young person from being included in the classroom
- Provide planned updates and maintenance to ensure assistive technology is in good working order and ready to use

- Install assistive technology apps and hardware conforming to a just-in-time capacity in line with the dynamic working practices of the school and needs of the students

1.7 Music Team Department

- Ensure that the children and young people have access to the music technology devices (bespoke iPads) that enable them to access classroom activities
- Rapidly support and correct music technology devices failures and configurations that would prevent the child or young person from being included in the classroom
- Provide planned updates and maintenance to ensure music technology devices including the teachers bespoke laptops are in good working order and ready to use
- Install music technology apps (iPads), software and hardware (Music specialist laptops) conforming to a just-in-time capacity in line with the dynamic working practices of the school and needs of the students

Identified Practitioners being Amy Wright / Marc Viera / Charlie Danger / Franz Allard / Scott Harris

1.8 All staff and volunteers working within the regulated area of the school

All staff, including contractors and agency staff, and volunteers are responsible for:

- Understanding & the implementation of policy
- Recognising that for our school staff are the first line of protection (not the internet filter)
- Attendance at safeguard training / learning from incidents
- Correct use of a personal electronic device for work requirements (regulated area zone 1) and should not be in a presence of a child unless in an emergency
- Correct use of a personal electronic device within unregulated area e.g., buttery, and if children are present ensure they are not able to overhear or see anything inappropriate.
- Ensuring the child has daily safe access to essential devices (within education and across leisure)
- Ensure update to apps are raised to identified school practitioners
- Ensuring child/family/residential house are resourced for the safe remote delivery of education
- Having an active role in creating a safe environment in which children can learn
- Providing appropriate learning opportunities to teach and reinforce online safety
- Providing the adequate staff supervision of children who can independently/ semi-independent navigate IT devices/technologies. If a young person accesses inappropriate material, an IRAR must be logged, DSL and Head of It & Transformation informed so further safety measures are put in place.
- Informing and work with the Lead DSL to ensure that any online safety incidents are logged (IRAR) and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are dealt with appropriately
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’
- Reflecting on learning from online safety incidents, implement actions to reduce further risk

- Keeping themselves safe online (i.e., not sharing passwords / writing passwords down / creating online logins for others)

1.9 Parents

- Notify a member of staff or the Head of School of any concerns or queries regarding online safety.
- Work with staff on the best & safe delivery of virtual learning
- Parents can seek further guidance on keeping children safe online by attending our internal virtual parent meetings / read material on TCT website and source advice & information on from further organisations and websites, such as:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- External information Healthy relationships – Disrespect Nobody
- Internal Information – located on school website/schoolzine platform

1.10 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 policy, when relevant, and expected to read and follow it.
- Use personal electronic devices correctly - The school is a regulated are and classed 'zone 1' the use of a personalised electronic device by a visitor is prohibited. It is the responsibility of the visitor to keep mobile phones on silent/vibrate whilst in the school.
- Notify a member of school management team / Lead DSL of any concerns or queries regarding online safety.

2. Process /Procedure

2.1 Educating children and young people about online safety

All the children are monitored for internet usage.

We provide support, teaching, and checks to ensure content is age respectful, that considers chronological age alongside the cognitive stage of development.

Most of our pupils, due to their need, are more vulnerable and are reliant on adults for most areas of their life. Therefore, placing the adult in the first line of protection against online safety (all 4 areas of risk) is essential. The regulatory of staff online training & learning about incidents is paramount in keeping the children safe.

Our curriculum (IMPACTS) has an environmental control technology strand (ECT) however online resources supplement the teaching across all subjects and key stages. In the planning of sessions adults source age respectful **content**. Material sourced & downloaded safely is vetted by the adult planning the session.

Our more formal/concrete learners require explicit teaching regarding online safety.

- Within **content** they may not understand terminology as require explanation on 'blocks' & suitable times to watch or listen to chosen age respectful shows.
- Within **contact** the learner beyond IMPACTS curriculum may not necessarily understand online friendships – they are used to adult intervention, and it can place them in a position of trusting everyone. The RSE policy outlines teaching.
- Within **conduct & commerce** the learner beyond IMPACTS curriculum do use devices with reduced supervision. They are more susceptible to meeting a person online therefore risk of being bullied (recognizing being bullied) through the internet.

2.2 Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our newsletter, website, or virtual meeting platform.

The school does send individual information on specific apps/tools for a specific child to use at home or on residential setting i.e., safe 'gaming'

If a child requires virtual learning the school will ensure that the parents are familiar with best practices. Including: -

- Before the virtual call, inform the parent/carer of the required information for the call to take place (session name/ date/ time / lead person)
- We ask the parent/carer to be present and help with the delivery of the session.
- We do not record the session.
- If anyone at home is inappropriately dressed, the virtual call will stop and resume later
- If a safeguarding concern is raised during the session, the DSL to be informed immediately.
- The school has several pre-recorded videos to minimize online risk. These are located on school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

2.3 Educating staff about online safety

To help prevent any online safety incident (including cyber-bullying & PREVENT) we will ensure that staff, and volunteers are appropriately trained in the recognition of the 4 category areas of risk. 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 7 minute bitesize)

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.

The school will actively discuss areas of risk with staff, volunteers, explaining the reasons why it occurs, the forms it may take at the Children's Trust School and what the consequences can be. Staff will understand that technology is a significant component in many national safeguarding and wellbeing issues and that all children are at risk of online abuse.

The IT department will update school staff on the various security measures that are in place to ensure the TCT network is safe from potential harmful contents. Also safe from viruses and cyber-attacks.

All staff maintain attitude ‘it could happen here’

By way of this training, all staff will be made aware of the facts that:

- Children and young people can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff to:

- exercise professional curiosity
- recognise contextual safeguarding and the potential harm beyond their families/TCT site
- develop better awareness to assist in spotting the signs and risks of online abuse for all our learners
- to intervene and escalate concerns – if there is any concern staff must act immediately
- develop the ability to influence children and young people to make the healthiest long-term choices and keep them safe from harm

The DSL and deputy/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.

2.4 Staff (DSL led) 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 children and young peoples’ 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, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a children or young person discloses that they are being abused and that this abuse includes an online element.

Any searching of children and young people will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on TCT electronic devices will be dealt with through the organisation's complaints procedure.

2.5 Acceptable use of the internet in school

All staff are expected to sign the annual Code of Conduct which includes the acceptable use of school's ICT systems and the internet.

All parents, volunteers and governors are expected to read policy regarding the acceptable use of the school's ICT systems. Internet and mobile phones.

Visitors will be expected to read and agree to the school's terms on 'use of mobile phones in our school' A full copy of the policy is available at school reception.

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.

If anyone has a concern about inappropriate use – no matter how small – it must be raised with the Lead DSL / school management.

The IT department can monitor the websites visited by children and young people, staff, volunteers, governors and visitors (where relevant) using TCT internet and Wi-Fi networks to ensure they comply with the above. More information is set out in the ICT acceptable use 2020 & Use of electronic communication devices 2019

2.6 Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password protected as outlined in the IT User policy
- Making sure the device is locked if leaving inactive for a period of time
- Not sharing the device among family or friends
- Ensure the device has anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates for TCT laptops/desktops and Windows based machines

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Helpdesk at The Children's Trust.

2.8 Security rules for home working:

We understand that there are risks associated in home and remote working that could lead to harm or distress to individuals and cause reputational damage to the school. As a school we will need to:

· Try not to take hard copy paperwork home unless necessary

· Do not take any originals of documents

· If work is taken home, it should be transported securely, i.e. – using Onedrive or where necessary an encrypted USB or portable hard drive

· Use strong passwords and do not share them with anyone.

· We advise our teams not leave your computer equipment logged in and unattended

2.10 How the school will respond to issues of misuse

Where a child or young person misuses the school's ICT systems or internet, we will follow the procedures set out in our staff code of conduct. 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 code of conduct. 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.

2.11 Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be obtained from the organisation IRAR system.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the eduactaional governance committee. The 360 review will be supported by an annual risk assessment that considers and reflects the risks children and young people face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1 – Stakeholder Engagement Checklist

Review and complete the following checklist to indicate which stakeholders were consulted in the development of this policy.

#	Question	Yes/ No	Stakeholder(s) to be consulted

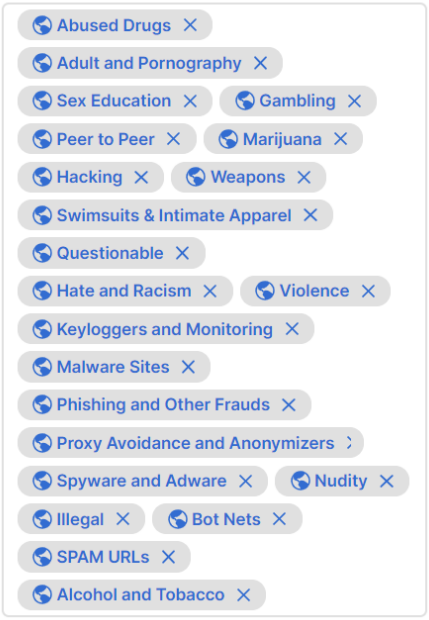
1	Is there a statutory requirement to have in place this particular policy/ does the policy need to comply with detailed legislation?	Y	Audit, Risk and Governance team
2	Is implementation of the policy (or any element of it) dependent on the use of new or existing information technology?	Y	Head of IT & Transformation
3	Does implementation of the policy (or any element of it) place any demands on/ or affect the activities of the Estates and Facilities teams (e.g. does it impact the provision or maintenance of premises, equipment, vehicles or other TCT assets)?	N	Head of Estates
4	Does implementation of the policy or any element of it involve/ impact the processing of personal data?	Y	Data Protection Officer
5	Does implementation of the policy require significant unbudgeted operational or capital expenditure?	N	Finance Director
6	Does implementation of the policy (or any element of it) directly or indirectly impact on the delivery of services / activities in other areas of the organisation? E.g. a policy written by a clinical lead in CF&S might impact on the delivery of care for CYP attending the School.	Y	Teachers / Leaders of Learning delivering learning sessions
7	Is there a need to consider Health and Safety or potential environmental impacts in developing and implementing the policy?	N	Health and Safety Manager
8	Have you consulted with a representative of those who will be directly impacted by the policy?	Y	Assistive Technology Team Environmental Control Subject Specialist Team Music Subject specialist Team
9	Is there a need to consider Equity, Diversity and Inclusion in developing and implementing the policy?	Y	EDI lead / rep for school – Maz Hanlon
10	Is there a need to consider sustainability and potential environmental impacts in developing and implementing the policy?	Y	Lead for Responsible Organisation
11	Please detail any other stakeholder groups consulted, if applicable.	Y	Family (virtual platform & schoolzine article) and Child (staff advocate)

Appendix 2 – TCT categories of blocks

On the TCT Firewall, affecting all TCT WiFi and internet traffic

Block

Content categories



Blocked on Sophos Endpoint Protection (installed on TCT laptops/desktops/surface Go devices)

NAME	ACTION
Adult/Sexually Explicit	Block
Alcohol & Tobacco	Block
Criminal Activity	Block
Hacking	Block
Illegal Drugs	Block
Intimate Apparel & Swimwear	Block
Intolerance & Hate	Block
Proxies & Translators	Block
Sex Education	Block
Tasteless & Offensive	Block
Violence	Block
Weapons	Block

Universal Guidance for Data Protection on AT Devices

Measures in place	Why bother?
AT devices labelled with a TCT number can only be used by that young person	As that device has personal data about the young person. It must be returned to the AT team for data wipe before it can be repurposed.
Any device used by multiple young people must be supervised use only.	You cannot know what someone put on a device if you leave it unsupervised. Data is not just photographs, videos, and account names. It is also history saved by apps, calibration data, voice data on Siri Alexa Cortana etc.
Never use an account with multiple users if that platform will suggest contacts. For example, skype, facebook, etc	The contact details of the other parties interacting with that account can easily become known to each other and to the user and this is a data breach. Individuals should use their own accounts.
Never create an account for an individual user. For example, email, skype, zoom, etc	If you create an account for a vulnerable person and later that account is involved in a data breach or exploitation, then TCT (and possibility you) could be held responsible. Always ask the young person or their family to create their own accounts. If they need help with this, please direct them to the AT Team for support.
When possible, **use the web version rather than app version** of services like email skype zoom etc.	This means less personal data on TCT devices. For example, the skype link on the house computers opens skype in a web browser not the app.
If you assist a young person to sign into a personal account, remember to **sign them out when done**.	If you leave them signed in, another person can access their info as a result of your action.
Never leave anything with personal information about a young person somewhere that anyone can access.	If you need to save something with personal information, you should do this in a password protected area. If you need help with this, contact the AT Team.
Never share passwords. This includes writing passwords on or near a device.	If there is a password that means something is being protected.

If there is accidental sharing of data by way of equipment TCT own or manage or by accounts TCT staff have created, TCT are responsible for any subsequent data breach on that device or account. Furthermore, if you take an action that violated TCT protocol and it results in a data breach, you could also have personal responsibility. #onlinesafety #safeguarding #infogovernance

PROBLEMS & QUESTIONS

Contact any member of therapy staff or the Assistive Technology Team on Extension 8645 or on GroupAssistiveTechnology@thechildrenstrust.org.uk

Written by: Marc Viera and Amy Wright, March 2020