Online Safety Policy

At present the children at TRACKS do not have internet access. If this should change then this policy will be fully reviewed.

When mentioned within this policy "Tracks network" relates to the SharePoint and OneDrive environment within Office 365.

This policy should be read in conjunction with the acceptable usage policy and the Data protection policy, GDPR, which all impact on the use of technology.

Breaches

A breach or suspected breach of policy by Tracks staff, trustees, volunteers result in the temporary or permanent withdrawal of Tracks ICT hardware, software or services from the offending individual. For staff any policy breach is grounds for disciplinary action in accordance with the Tracks disciplinary procedure. Where the policy is covered by statute this may also lead to criminal or civil proceedings.

The GDPR policy states acceptable use of information, storage of that information and how long data can be kept (please see separate policy).

Managing email

In the context of TRACKS, email should not be considered private.

Staff and Trustees should use a Tracks email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that Trustees are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

- TRACKS gives all staff and Trustees their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Staff and Trustees should use their Tracks email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact children, parents or conduct any school business using personal email addresses.
- E-mail is not a secure and as such confidential information should be transferred using secure or encrypted programs such as Herts FX
- E-mails created or received as part of your work at TRACKS will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Staff must inform a member of the senior team, if they receive an offensive email.
- If sensitive information must be sent by email it should at the very minimum be password protected. The password can be supplied to the recipient by another method.

Incident reporting
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to a member of the senior team. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Principal.

Managing the internet
All use of the internet at **TRACKS** is regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

- TRACKS ensures children will not have access to the Internet.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is the Principal's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Staff are aware that TRACKS based email and internet activity can be monitored and explored further if required.
- TRACKS does not allow children access to internet logs.
- If staff discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of the senior team.

Password security
Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.

Personal or Sensitive Information

Protecting Personal or Sensitive Information
Staff, Volunteers and Trustees will;

- Ensure that any information accessed from their own PC or removable media equipment is kept secure and removed any portable media from computer when not attended.
- Ensure they lock their computer screen when leaving it unattended.
- Ensure accuracy of any personal or sensitive information you disclose and is not disclosed to any unauthorised person.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use.

17. Safe use of images
17a. Taking of Images and Film

- TRACKS seek written permission from every family regarding taking or storing images of any member of the TRACKS community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of the children) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Children are not permitted to use personal digital equipment, including mobile phones and camera, to record images of others, this includes when on outings. However, with the express permission of the Principal, images can be taken.
- All images are taken using ipads and then uploaded to Tapestry (which is GDPR compliant). All parents have constented to these photos being used for this purpose.

17b. Consent of adults who work at the school
Permission to use images of staff who work at the school must be sought before images are used.

17c. Publishing pupil's images and work
On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the TRACKS web site and Facebook page.
- in the TRACKS prospectus and other printed publications that TRACKS may produce for promotional purposes
- in display material that may be used in TRACKS Early Years Centre
- in display material that may be used in external areas, i.e. exhibition promoting TRACKS
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time.

Children's names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Children's full names will not be published. Before posting children's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

E-Safety

- i-pads are used within the classroom by staff only. These devices are used only for taking photos and videos of children to be uploaded to Tapestry.
- We acknowledge that adults play an essential role in helping young children learn the foundation of using technology safely.

- Whilst we acknowledge do not access to technology within our setting, they will likely to be using at home. It is an adult's responsibility to enable children to use technology safely.
- Children in our setting do not have access to the internet.
- Photos and videos are uploaded directly to Tapestry for parents' information. All parents have signed consent forms and agreed not to share any photos that contain other children with outside sources.

Storage of Images

- Children and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Principal
- Rights of access to this material are restricted to the teaching staff and children within the confines of the school network.

School ICT Equipment including Portable and Mobile ICT Equipment and Removable Devices.
School ICT Equipment

- As a user of Tracks ICT equipment you are responsible for your activity.
- Visitors will not be allowed to plug their ICT hardware into the school network points. They must be directed to the wireless facilities for visitors.
- Ensure all ICT equipment is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- Personal or sensitive data should not be stored on the local drive or desktop PC, laptop, USB memory stick or other portable device.
- Privately owned ICT equipment will not be used on the Tracks network.

Portable and Mobile ICT Equipment

This covers items such as laptops, mobile devises and removable storage devices.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physical secure in accordance with this policy to be covered for insurance purposes.
- Portable equipment must be transported in its protective case if supplied.

Mobile technologies

This covers the use of mobile phones and other portable devices such as tablets.

At TRACKS autism the welfare and well-being of all our pupils is paramount. This policy on the use of mobile phones in school has been drawn up in the best interests of pupil safety and staff professionalism.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used, in turn eliminating the following concerns:

1) Staff being distracted from their work with children
2) The inappropriate use of mobile phone cameras around children.

The policy is to safeguard both children and adults as any adult found with a mobile phone other than the setting phone is vulnerable to accusations

This policy applies equally to mobile phones, smart watches and other devices and links to the technology and Data Security policies. (All communication devices herein after as mobile phones.)

Staff:

- Personal mobile phones must be left in lockers, their bag or in the office at all times. Staff must not make personal calls/texts during session times unless on an authorised break, away from the children.
- Anyone expecting an emergency call should inform the manager/give the pre-school number as a contact, and the manager will ensure that the call can be taken away from the children.
- If staff have a personal emergency, they are free to use the office phone or make a personal call away from the classroom with the Principal's permission.

Staff need to ensure that the Centre Manager has up to date contact information and that staff make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff member.

- All parent helpers/students/volunteers will be requested to place their bag containing their phone in the office or other appropriate location. Mobile phone calls may only be taken at breaks or in their own time away from the classroom.
- Mobile phones must not be used under any circumstances to take photos in the setting/of the children, and any member of staff discovered doing this will be the subject of disciplinary proceedings immediately.
- The setting's iPads may be used to take photos of children (with the parent's prior consent, recorded in their personal file). These images should be used for uploading to Tapestry if consent is given by parents.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Principal or Centre Manager.
- Staff must not accept parents of children within the setting as 'friends' on Facebook or any other social networking site. Parents will be informed at their child's induction that this is a policy of the setting.
- Where a member of staff uses a social networking site of any kind they must not discuss the setting, their colleagues, management, children or families, ensuring that they respect confidentiality at all times, and that they do not say/discuss anything which could bring the pre-school, its management, their colleagues, children or families into disrepute, or damage the reputation of the setting in any way. They should also be aware that personal photographs/posts/comments, which portray the member of staff in a way that may compromise their position within the pre-school should not be posted, and that their privacy settings are maintained so that parents/the wider community, cannot access any such photos/posts/comments. Any member of staff discovered not adhering to this will be the subject of disciplinary proceedings immediately which may lead to dismissal from their position.

- TRACKS is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the TRACKS community is not allowed.
- Users bringing personal devices into TRACKS must ensure there is no inappropriate or illegal content on the device.

Parents & Carers:

- In the event of an unplanned closure (i.e. snow closure or a heating failure) TRACKS will send each family a text message/phone/email informing them of the change of circumstances. It is therefore imperative that parents supply school with at least one up-to-date mobile number.

Parents & other visitors:

- We request that parents do not use mobile phones in the school building or grounds.
- Mobile phones must never be used to take photographs in the school building or grounds.

We very much appreciate our parents' support in implementing this policy in order to keep your children safe.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social medial are an important part of our daily lives.

- Tracks uses Facebook to communicate with parents and carers.
- Staff are not permitted to access their personal social media accounts using school equipment.
- Staff, Trustees, volunteers, children, parents and carers are aware that their online behaviour should at all times be compatible with UK Law.

Complaints

Complaints relating to the use of technology should be made to the Principal.

This policy was adopted by	TRACKS autism	*(name of provider)*
On	February 2023	*(date)*
Signed on behalf of the provider		
Name of signatory	Alexa Pickergill	
Role of signatory (e.g. chair, director or owner)	Chairperson	