Online Safety Policy

Current version:	V1
Team:	Safeguarding
Owner:	Director for Safeguarding
Author:	Arwen King
Date effective from:	10/11/2023
Date of last review:	10/11/2023
Date of next review:	01/04/2026

Record of changes

Version	Date	Changes

Company number: 10755829

Introduction

The Outdoor Group (TOG) is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Definitions

The Outdoors Group (also known as 'TOG' or 'the company') is comprised of 3 areas of business: The Outdoors School, Forest School and Training, and Transitional Learning Programme.

This Policy cover all aspects of the company's work with learners and parents/carers.

Purpose

Technology have become integral to the lives of children and young people. They are an essential resource to support teaching and learning. Children and young people have an entitlement to safe access to existing, new, or developing technology. It is impossible to eliminate all risk entirely, therefore we must educate children and young people so that they have the knowledge, skills, and confidence to keep themselves safe. Such knowledge should also recognise the potential for excessive use, which may impact on social and emotional learning and development.

This Policy is used in conjunction with other relevant following group policies such as:

- Safeguarding and Child Protection
- Relationship and Sex Education
- Behaviour & Anti Bullying
- Data Protection
- Curriculum Statement

Whilst at school or attending other TOG sessions, learners should only access ICT supported learning on TOG devices connected to the site Wi-Fi network. Personal devices such as laptops are not normally permitted.

Scope

The Outdoor Group will ensure safeguards are in place to prevent access to inappropriate web content or activity. However, we must acknowledge and understand that learners will have access to the internet outside of our sites and must be educated accordingly.

Currently the internet technologies children and young people are using both inside and outside of the learning sessions include, but are not limited to:

- Websites.
- Microsoft Teams
- Microsoft Edge
- Other Learning Platforms and Virtual Learning Environments.
- Email and Instant messaging.
- Blogs and Wikis.
- Podcasting.
- Video Broadcasting.
- Music Downloading.
- Gaming.
- Mobile/ Smart phones with text video and web functionality.
- Other mobile devices with web functionality.

Whilst exciting and beneficial, many of the internet technologies list above are not well policed by regulatory bodies. All users need to be aware of the range of risks associated with their use.

Roles and Responsibilities

At the Outdoors Group we understand the responsibility to educate our learners on e-Safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe and legal when using the internet and related technologies in and beyond the context of the classroom. e-Safety is an important aspect of leadership within The Outdoors Group, and the Senior Leadership Team have ultimate responsibility for ensuring that this and relevant related policy and practice are embedded and monitored.

E-Safety skills development for staff

New staff receive information on the Group's approach to e-Safety and relevant policies as part of their induction.

All staff are made aware of individual responsibilities relating to the safeguarding of children/young people within the context of e-Safety and know what to do in the event of misuse of technology by any member of the staff community.

All staff are encouraged to incorporate e-Safety activities and awareness within their teaching.

E-Safety in the Curriculum

ICT and online resources are increasingly used across our programmes. It is essential for e-Safety guidance to be given to learners on a regular and meaningful basis, and we continually look for new opportunities to do this.

If we are forced to pause onsite attendance for any reason, we will continue education through our virtual classroom which currently uses the Microsoft Teams platform. It is important for the social and emotional wellbeing of our learners that we remain connected during any period of closure. It is even more important that learners feel safe and free from harm during this time.

At all times the members of staff will remain vigilant about any form of cyber-bullying or prejudice-based bullying. Our online portal must not be seen as a place where learners can behave any differently to their expected behaviour in school or any of our sessions.

During any online/off site learning, sanctions for inappropriate use are shared with learners so they are aware of the need for kindness and tolerance.

Sanctions for Online Behaviour

Staff and learners must respect the principles of politeness, respect, and kindness. Any communications found to be disrespectful, offensive, hurtful or in any way having a detrimental effect on a learner or staff member's well-being, will be robustly and immediately addressed.

A member of staff leading a virtual learning session will inform a learner if their behaviour is inappropriate and give them the opportunity to rectify it immediately and apologise if required. Learners are encouraged to speak openly if they feel another learner is not acting appropriately.

If the behaviour causing concerns continues the learner responsible will be immediately removed from the virtual learning session. The member of staff leading the session will immediately explore what further action should be taken to support the learner responsible and/or impose sanctions. The member of staff can seek support to do this from the SENDCo or any member of group's Senor Leadership Team. Full factual details of what happened, and any action taken must be recorded. The Parent/Carer of the learner responsible will be informed. Where appropriate the parent/carer of any learner affected will also be informed (this will be at the judgement of the member of staff leading the virtual input or the Senor Leadership Team).

Educating the learners on the dangers of technologies that may be encountered outside our school or other TOG sessions is done as opportunities arise. Any incidences relating to sexual harassment are discussed at a regular safeguarding staff briefing and any necessary action led by our Designated Safeguarding lead or their nominated representative/deputy.

Learners are made aware of the impact of online bullying and are advised how to seek help if they are affected by these issues. In all times, learners are encouraged to treat technology in the same way as face-to-face relationships and that these should be conducted in a place of safety, free from harm and persecution.

Password Security

Password security is essential for staff as they access and use personal data. All personal data is kept securely on company systems and each staff member has their own log in. All staff are expected to keep their password secure and change it regularly or immediately if they suspect their password is known by another. Staff must not give learners access to secure company systems and should take all reasonable steps to ensure learners do not have sight of passwords for such systems.

Data Security

Access to and appropriate use of company data is taken very seriously, and any such access or use must comply with Data Protection legislation and related policies and procedures.

- Staff are aware of their responsibilities when accessing company data/personal data.
- Data is stored on secure systems which are GDPR compliant.
- All guidelines relating to Data Protection must be followed.

The Internet

The internet is an open communication medium, that is always on and is available to all. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction as well as a potential risk to young and vulnerable people. Any suspected or actual inappropriate use detected will be investigated.

TOG has secure filtering software in place, to prevent learner or staff access to inappropriate web content. This software has been specifically developed for learners' use and has been successfully used over time.

Tracking

All staff and learners have individual ICT accounts and passwords. Staff and learners must be logged into their account to access any school activity that is ICT based and/or browse the internet.

Our filtering software monitors any attempt to access inappropriate content and can provide a detailed report of such activity. Software allows both identification of any individual attempting to access something inappropriate and what they were trying to access. Activity is monitored by CF Systems and concerns shared with the Head of Pastoral or relevant tutor for appropriate action.

TOG recognises that no software solution can offer 100% guaranteed protection. Staff will remain vigilant and will immediately report any suspected bypassing of filtering software by a learner/staff member or access to any inappropriate website that filtering software does not appear to recognise and block. CF Systems will be immediately made aware of any such concerns so they can take any action needed to prevent a repeat.

Anti-Virus Protection

TOG will ensure appropriate anti-virus software is installed on all company technology.

TOG's anti-virus software auto updates content so no specific action should be required by staff or learners to ensure a device has the latest version in place.

Additional Safeguards

- TOG will ensure learners have supervised access to Internet resources.
- Staff will preview any sites before use.
- All users must always observe copyright.
- If staff or learners discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately.
- Learners are not able to download programs or apps on company-based technologies.
- Written permission from parents is obtained as part of the induction process, to use images or videos of the learner on the website and social media platforms. Full names are never used.

Managing Other technologies

We recognise the importance of encouraging our learners to think carefully about the way that information can be added and removed by users of these sites.

- Access to social networking sites for personal use is blocked to all learners.
- All learners are encouraged to be cautious about the information given by others on websites.
- Learners are reminded to avoid giving out personal details on such websites which may identify them or where they are (full name, address, mobile /home phone numbers, learning environment, IM/email addresses etc, location services)
- Learners are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Learners are asked to report any incidents of e-bullying to the staff.
- Staff use of social media
- TOG staff will not invite, accept, or engage in communications with parents or learners from the learning community on any personal social media whilst in employment at TOG.
- Any communication received from learners on any personal social media sites must be reported to the Head of Pastoral or Line Manager. Staff must block the learner to prevent further contact.
- If any member of staff is aware of any inappropriate communications involving any learner on any social media, these must immediately be reported as above.
- Members of staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- Staff should not use personal email accounts or mobile phones to contact members of the learning community on company business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher or Senior Leadership Team.
- Staff are strongly advised to avoid posts or comments that refer to matters relating to TOG and members of its community on any social media accounts.
- Staff should not accept any current learner of any age or any ex-learner of The Outdoors Group under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Staff must not represent personal views as those of the company in any social medium.
- Staff must not use social media and the internet in any way to attack, insult, abuse or defame learners, their family members, colleagues, other professionals, other organisations, or TOG.
- Personal Mobile Devices (including phones)
- Please see The Outdoors Group Policy on use of personal devices.

- The company is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the company community is strictly prohibited.
- Users bringing personal devices into company sites must ensure there is no inciting, inappropriate or illegal content on the device.

Managing email

The use of email is an essential means of communication for both staff and learners. In the context of the company, email should not be considered private.

- All email communication between staff and members of the Outdoors Group community regarding company business must be made from an official Outdoors Group email account. This is to minimise risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. Under no circumstances should staff contact learners, parents or conduct any business using personal email.
- Emails sent to an external organisation should be written carefully before sending, in the same way as a letter written on company headed paper.
- Learners may only use company-approved email accounts when logged into our systems and only under direct teacher supervision and for educational purposes.
- The forwarding of chain letters is not permitted.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others, or arranging to meet.
- Learners must immediately report abusive or offensive emails to staff / trusted adult.
- Staff must inform the Head of Pastoral or Line Manager if they receive an offensive or abusive email.

Safe use of images

Digital images are easy to capture, reproduce and publish and therefore misuse. We must remember that it is not appropriate to take or store images of any member of the learning community without first seeking consent and considering the appropriateness.

- With the written consent of parents/carers (on behalf of learners) the company permits the appropriate taking of images by staff and learners using company devices.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of the learners.
- The Headteacher/Site Lead reserves the right to confiscate any mobile device being used inappropriately.

Publishing a learner's image and/or work

On a learner's entry to The Outdoors Group, parents/carers will be asked to give permission to use their child's work / photos in the following ways:

- On The Outdoor Group website and any related official social media
- Company prospectus
- Company newsletters
- Company display boards
- Local and national press

This consent form is considered valid for the entire period that the learner attends TOG unless the parent/carer withdraws permission in writing. Learner names will not be published alongside their image.

Storage of images

- Images / films are stored on secure systems.
- Learners and staff are not permitted to use personal portable media for the storage of images without the express permission of the Headteacher or Senor Leadership Team.
- Rights of access to this material are restricted to teaching staff within the confines of the Company network. Certain photo albums may be shared between learners and staff for work purposes.

Misuse and infringements

Complaints should be made in accordance with our Complaints Policy and Procedure.

If staff behaviour whilst using social media interferes with their job (such as if they are on social networking sites during a time when they are at work/on duty), has harmed or could potentially harm the Outdoors Group reputation, or is

implicated in any other way which could be considered a disciplinary matter, then staff misconduct and disciplinary process will be applied. Depending upon the severity of the situation, actions could include dismissal and police involvement.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher and Senior Leadership Team.

Deliberate access to inappropriate material by any user will lead to the incident being logged, reported, and investigated. Other agencies such as the police will be involved if necessary.

Learners with additional needs

The company endeavours to create a consistent message for parents/carers of all learners and this in turn should aid establishment and future development of the e-Safety policy.

Staff are aware that all our learners may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a learner has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these young people.

Staff - Acceptable use and conduct

ICT and related technologies such as email, the internet and mobile devices are an expected part of our daily working life at The Outdoors Group. This policy is designed to ensure that all staff are aware of their professional and personal responsibilities when using any form of ICT. All staff are expected to fully adhere to this policy and its content.

Any member of staff needing clarification on any point of policy or approach should contact the Headteacher or Head of Business Area.

Staff agree that they will:

- Only use the company's email, Internet, and any related technologies for professional purposes or for uses deemed 'reasonable'.
- Comply with ICT system security and not disclose any passwords.
- Ensure all electronic communications with learners and staff are compatible with their professional role.

- Not give out any personal details, such as mobile phone numbers or email addresses to learners.
- Only use an approved company email account for any company business.
- Ensure that personal data is kept secure and is used appropriately.
- Not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory.
- Ensure images of learners and/or staff will only be taken, stored, and used for professional purposes in line with the e-Safety policy and with written consent of the parent, carer, or staff member.
- Not use any personal device to record images of learners and staff.
- Respect copyright and intellectual property rights.
- Ensure their online activity, whether at the school, at other TOG sites or elsewhere, will not bring their professional role or the company into disrepute.
- Support and promote the e-Safety policy and help learners to be safe and responsible in their use of ICT and related technologies.