



E-Safety Policy

Written by Lorraine Squires Shaw (director)

Date: 12th October 2022

Review Date: October 2024

Purpose

This policy is written to ensure all Staff, Parents and students are fully aware of the purpose and nature of the e-safety policy.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter.

New Leaf Triangle will endeavour to highlight benefits and risks of using technology and provide safeguarding and education for users to enable them to control their online experience.

The responsibility for managing e-Safety can be challenging and so this document aims to set out procedures to be followed to minimise what can be a difficult process.

Links to other policies and national guidance

The following policies and procedures should also be referred to

- Safeguarding Policy
- Whistleblowing Policy
- Positive behaviour support policy
- Staff Code of Conduct
- Data Protection Policy

The following local/national guidance links to this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2020
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our communities, lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just in schools and education provision but outside as well, and we will endeavour to help prepare our students to safely benefit from the opportunities the internet brings.

- We will discuss, remind or raise relevant e-Safety messages with students wherever suitable opportunities arise during sessions; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be planned to ensure that it is age appropriate and supports the learning objective for specific topics.
- When searching the internet for information, students will be guided to use age appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.
- Students will be made aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as NSPCC.

Staff Training

Our staff receive information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the E Safety Policy, e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of any misuse of technology.
- All staff will be encouraged to incorporate e-Safety activities and awareness within their sessions.

Managing Access to the internet

- Laptops and tablets are not freely accessible to students and are only used as a planned part of sessions.
- All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

E-Mail

- Staff should only use approved email accounts allocated to them by New Leaf.
- Staff should not use personal email accounts for professional purposes, especially to exchange any New Leaf related information or documents or to email parents/carers.

- Staff should not send personal emails to students, but may be required to send work related emails such as course work, resources etc.
- Students are encouraged to immediately tell a member of staff if they receive any inappropriate or offensive emails.
- Irrespectively of how students or staff access their email (from home or at New Leaf), our New Leaf policies still apply.

Social Networking

- Staff will not post content or participate in any conversations which will be detrimental to the image of New Leaf. Staff who hold an account should not have parents or students as their 'friends'. Doing so will result in disciplinary action or dismissal.
- Blogs or social media sites should be password protected and run from the New Leaf Website with approval from Directors.

Students Publishing Content Online

- Students will not be allowed to post or create content on sites unless the site has been approved by a director.
- Students' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of students must be stored on the New Leaf drive and not on personally owned equipment.
- Students and staff are not permitted to use portable devices to store images/video/sound clips of students. They must all be uploaded to the New Leaf drive.

Mobile Phones and Devices

General use of personal devices

- Mobile phones are needed by staff to ensure good communication and safety in an outdoor learning environment.
- Images or videos taken on mobile phones must be uploaded to the New Leaf drive on the day they are taken and deleted from devices.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Students' use of personal devices

- Students who need to bring a mobile phone in to New Leaf are permitted to do so.
- The phone can be kept safely in a locked cabinet during the day if needed.
- Students should be encouraged not to use phones during their sessions wherever possible. However, we do realise that due to the nature of the conditions of some of the students we work with, their phones can be very important to them and offer a means of security and comfort and a distraction from anxiety.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if a staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt sessions,

NLT E-Safety Policy

- commit an offence,
- cause personal injury, or
- damage property

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- If a member of staff breaches the policy then disciplinary action may be taken.

CCTV

- New Leaf may use CCTV in some areas of the property as a security measure. This is not used for recording in the daytime.
- Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

General Data, Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on the NLT drive, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the New Leaf population and external stakeholders, particularly, but not exclusively: students, parents, staff and external agencies.

Personal and sensitive information should only be sent by email when on a secure network and sent with protection such as encryption or password protected.

Personal data should only be stored on secure devices. In the event of a data breach, New Leaf will notify the persons, LAs, schools etc concerned.

Authorising Internet access

- All staff must read this policy before using any of new Leaf's IT resources.
- All parents will be required to grant permission prior to their children being granted internet access.
- New Leaf maintain a current record of all staff and students who have been granted access to the internet.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we are located. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Lead). All students must be fully supervised when accessing the internet.

Sexual Harassment

