# Acceptable Use Policy (AUP)

Newtown National School
Address: Newtown, Ardee, Co. Louth.

## Rationale

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

## School's AU Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

## General

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The teachers and SNA's will monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

## World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials.
- Students will use the Internet for educational purposes only.
- Students will never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

## Email

- Students will use approved class email accounts under supervision by or permission from a teacher./parent
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher/parent

**Internet Chat**

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

**School Website**

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Website using facilities such as guestbooks, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details?
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website with out the parental permission. Video clips may be password protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

**Student Laptops and Tablets**

- Currently, there are 6 student laptops and 24 tablets for use within the classroom setting. Each laptop has been configured for student use. Parental Controls are enabled and student accounts are granted restricted access and control.
- An age appropriate and internet-safe browser Kiddle or KidRex has been installed as the default student browser on each laptop and tablet.
- In the event that a web browser is accessed (or granted access), the school has a content filtering system to block any attempts by users to access content deemed to be inappropriate for our students.

**Personal Devices**

Pupils may only use their own technology in school when prior permission has been sought and granted. Pupils using their own technology in school, - such as a mobile phone, sending text messages, or the unauthorized taking of images, still or moving is in direct breach of the school's acceptable use policy and the school's mobile phone policy.

## Distance Learning/ Direct Communication using Internet

Teachers in the school may choose to use a number of tools for classroom communication. Examples include Google Classroom, Webex, Zoom, SeeSaw, and ClassDojo. Some of these tools provide synchronous video opportunities whereby a staff member directly speaks to the children live - e.g. through a webinar or online meeting. The staff member invites pupils and their families to these meetings using a code, this code must not be shared. All meetings must be locked.

The following are ground rules for synchronous lessons online.

- All meetings will be password protected
- Two teachers must be present at all meetings
- All people involved in the meeting will conduct themselves in a similar manner that would be expected in a regular class.
- The staff member has the right to remove any person being disruptive from a synchronous lesson.
- A parent or authorised adult must be present when a pupil is engaging in a meeting. They should monitor all online interactions from the pupil.
- The chat facility must be disabled for all meetings
- Any interaction from a pupil that could be deemed as inappropriate may result in the child's removal from the lesson or, where appropriate, a referral to Child Protection services.

## Cyberbullying

Understanding Cyber Bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse another person.
- It can take place anywhere and can involve many people.
- Anybody can be targeted, including pupils, school staff, and members of the wider school community.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, and unauthorised publication of private information or images.

There are many types of cyber-bullying. The more common types are:

- Text messages – can be threatening or cause discomfort. Also included here is 'Bluejacking' (the sending of anonymous text messages over short distances using Bluetooth wireless technology)
- Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls, abusive messages or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.

- Chat room bullying – menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Instant messaging (IM) – unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
- Bullying via websites – use of defamatory blogs (web logs), personal websites, gaming websites, and online personal 'own web space' sites such as You Tube, Facebook, Ask.fm, Bebo, Twitter, SnapChat, and Myspace, among others.

Procedures for preventing Cyber Bullying:

- Staff, pupils, parents, and Board of Management (BOM) are made aware of issues surrounding cyber bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff CDP (Continuous Professional Development) will assist in learning about current technologies.
- Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies, Friendship Week activities and other curriculum projects.
- Pupils, parents, and staff will be involved in reviewing and revising this policy as school procedure.
- All reports of cyber-bullying will be noted and investigated, in accordance with the school's Anti-Bullying, Mobile Phone, Child Protection, and Code of Behaviour where applicable.
- The school will engage a speaker Community Guard to facilitate a workshop on Internet Safety for 5th – 6th Classes and mark Safer Internet Day (SID) annually.
- Procedures in the school's Anti-Bullying and Child Protection policies shall apply.

**Legislation**

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

**Sanctions**

Misuse of the Internet may result in disciplinary action, in accordance with the school's Code of Behaviour. The school also reserves the right to report any illegal activities to the appropriate authorities.

**Support Structures**

Where appropriate, the school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet. Newtown NS has adopted the Child Protection Procedures for Primary and Post Primary Schools as part of its child protection policy. This policy has been made available to the Parents' Council and is available to all parents on request.

Websites offering support and advice in the area of Internet Safety:

- Webwise - http://www.webwise.ie/
- Safe Internet - http://www.saferinternet.org/ww/en/pub/insafe/
- Newtown NS website offers Cyberbullying and Internet Safety Guides for Parents

## Implementation

### a) Roles and Responsibilities

All teachers are responsible for the implementation of the AUP . In relation to distance learning parents share the responsibility.

### b) Time-frame

The implementation of this AUP  in our classes is ongoing

## Review

This policy will be reviewed in 2023 or as and when the need arises. A hard copy of this policy will be retained in the non - curricular folder and available for anyone wishing a copy of it.. It will also be uploaded on to the website.

## Ratification

This AUP  was sanctioned and ratified by the Board of Management.

Signed: John Lynch Date: 25th June 2020