E-Safety and Acceptable Use Policy

Thornfield House School

8-12 Jordanstown Road
Newtownabbey
Co Antrim
BT37 0QF
Tel: 028 9085 1089
Fax: 0289086 5543
Website: www.thornfieldhousesch.co.uk

Ratified by the Board of Governors

signed: _____

date: _____

To be reviewed: November 2023

Contents:

Thornfield House School ICT Vision

Thornfield House believes in the holistic development of the child to his / her potential. It will provide a broad, balanced and differentiated curriculum. ICT is fundamental to daily life, and is continually developing with new technologies emerging.

Our vision is to create motivated learners through the safe use of ICT to enhance and extend learning. Thornfield House School will endeavour to equip pupils with the basic skills to prepare them for a future in which ICT is an integral part of society.

This will be developed through the three '**I**'s:

· **I**CT skills of staff and pupils in school so that they are confident and independent users.

· **I**nteractive learning through a range of technologies.

· **I**ndependent learning for life.

Our vision encompasses the following aims:

· ICT will be embedded into every day school life by enabling pupils to explore, express, exchange, evaluate and exhibit their work.

· To provide opportunities to enable staff and pupils to be safe, confident, competent and independent users of ICT.

· To raise levels of teacher competence and confidence in integrating ICT into planning, teaching, assessment and levelling of pupil's work.

· To provide an environment where teachers and pupils have access to a range of ICT resources that can be used to support teaching and learning across the curriculum.

· To ensure that pupils use ICT with purpose and enjoyment whilst increasing motivation and confidence.

· To ensure pupils know how to stay safe online.

· To encourage thinking skills through the creative use of ICT.

· To become reflective and flexible users ICT.

Introduction

Thornfield House School encourages all our pupils to use the extensive range of online information resources available with pupil safety as a priority. At Thornfield House School we understand that while no filtering system can fully guarantee the restriction of unwanted material, we must equip our pupils with the skills to know how to stay safe online. We believe *'Schools have a duty of care to enable pupils to use on-line systems safely' (DENI circular 2013 / 25).* E-safety is a whole school issue and responsibility.

We recognise that '*Safeguarding and promoting pupils welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities' (Department of Education Online Safety DE Circular Number 2016/27). Furthermore, 'pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.' Department of Education Online Safety DE Circular Number 2016/27*

At Thornfield House School, we aim to encourage parental / carer involvement through shared resources and e-Safety information. Recommendations for parents and carers include using the TEAM framework:

· **T**alk frequently to children about staying safe online

· **E**xplore the online world together as a family

· **A**gree on family rules about what is and isn't OK online

· **M**anage privacy settings and controls on the sites, apps and games the family uses.

This policy links to the following policies:

· Safeguarding and Child Protection

· Pastoral Care

· Anti-Bullying

· PDMU

· Data Protection.

E-Safety Context

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the internet and Digital Technologies in Schools and DENI Circular 2011/22 and 2013/25 on Internet / e-safety. This document sets out the policy and practices for the safe and effective use of the internet and related technologies in Thornfield House School. It also links to Article 17 and Article 36 from the UN Convention on the Rights of the Child which states:

Article 17 (**Access to information; mass media**): Children have the right to get information that is important to their health and well-being. Governments should encourage mass media – radio, television, newspapers and **Internet content sources** – to provide information that children can understand and to not promote materials that could harm children. Mass media should particularly be encouraged to supply information in languages that minority and indigenous children can understand. Children should also have access to children's books.

Article 36 (Other forms of exploitation): **Children should be protected from any activity that takes advantage of them or could harm their welfare and development.**

E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing. This policy aims to provide an understanding of appropriate ICT use, as well as highlight the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions.

E-Safety in the school context:

· is concerned with safeguarding children and young people in the digital world;

· emphasises learning to understand and use new technologies in a positive way;

· is less about restriction and focuses on education about the risks, as well as the benefits, so that users feel confident online;

· is concerned with supporting pupils to develop safer online behaviours, both in and out of school; and

· is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Using the Internet for Education

The benefits include:

· Unlimited access to worldwide educational resources; including online assessment;

·Enhanced curriculum, with interactive learning tools;

· Rapid and cost effective communication;

· Interaction with people that they otherwise would have been unable to meet;

· Gaining an understanding of people and cultures around the globe;

· Greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others;

· Staff professional development through access to new curriculum materials, shared knowledge and practice.

The internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. Anyone can send messages, discuss ideas and publish materials with little restriction, some of which could be unsuitable. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

In school pupils will be taught what internet use is acceptable, what is not acceptable and will be given clear guidelines for internet use. During each school year, pupils will be taught lessons on e-safety to remind them the importance of keeping safe online. Where possible, outside agencies will be invited into school to discuss the importance of staying safe online. Appropriate resources and weblinks will be shared with staff through 'OneDrive'.

Risk Assessment

The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. With these opportunities, we also have to recognise the risks associated with the internet and related technologies. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Thornfield House School will take all reasonable steps to mitigate the risks identified below and ensure that users create and access only appropriate material. It is impossible to eliminate the risk completely, and is therefore essential through good educational provision to build pupils' resilience to the risks which they may be exposed. Pupils should have the confidence and skills to face and deal with scenarios which may arise. At Thornfield we aim to teach our pupils how to cope if they come across inappropriate material or situations online. This will be part of the teaching and learning of e-safety in the curriculum.

Potential risks / dangers for pupils using the internet (this list is not exhaustive):

· Access to illegal, harmful or inappropriate images or other content;

· Unauthorised access to/loss of/sharing of personal information;

· The risk of being subject to grooming by those with whom they make contact on the internet;

· The sharing/distribution of personal images without an individual's consent or knowledge;

· Inappropriate communication/contact with others, including strangers;

· Cyber-bullying;

· Access to unsuitable video/internet games;

· An inability to evaluate the quality, accuracy and relevance of information on the internet;

· Plagiarism and copyright infringement;

· Illegal downloading of music or video files;

· The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Network Access

Pupil access to the internet is through a filtered service provided by C2K, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Staff and pupils accessing the internet via the C2K Education Network will be required to authenticate using their C2K username and password. Access to the internet via the C2k Education Network is fully auditable and reports are available to Mr. Burns, School Principal.

All websites through the C2K filtering service are categorised as either red (unavailable) or green (available). By default all users are given access to a core set of green sites. In addition, users can be added into internet security groups, to provide further access. Access is controlled by the school principal and the C2K Managers within the school. If staff or

pupils discover any unsuitable websites or material, then the URL will be reported immediately to the schools ICT co-ordinator.

Cyber Bullying

Cyber bullying, as with any other form of bullying, is taken very seriously by the school. Pupils engaging in cyber bullying may be dealt with in line with the school's 'Anti-Bullying Policy'.

Cyber Bullying can take many forms, such as:

· Email—nasty or abusive emails which may include viruses or inappropriate content;

· Instant Messaging (IM) and Chat Rooms—potential to transmit threatening or abusive message perhaps using a compromised or alias identity;

· Social Networking Sites—typically includes the posting or publication of nasty or upsetting comments on another user's profile;

· Online Gaming—abuse or harassment of someone using online multi-player gaming sites;

· Mobile Phones—examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;

· Abusing Personal Information—may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber bullying can constitute a criminal offence. While there is no legislation for cyber bullying, the following may over different elements of cyber bullying behaviour:

· Protection from Harassment (NI) Order 1997
http://www.legislation.gov.uk/nisi/1997/1180

· Malicious Communications (NI) Order 1988
http://www.legislation.gov.uk/nisi/1988/1849

· The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber bullying to parents first and the school and, if appropriate, parents contact the PSNI to ensure the matter is properly addressed and the behaviour ceases. The school will also keep a record of cyber bullying incidents, if they have occurred within school.

Acceptable Computer Use

The C2K computer system is owned by the school and is made available to staff their professional activities including teaching, research, administration and management. The school's e-safety policy has been drawn up to protect all parties—the pupils, the staff and the school. The school reserves the right to examine and delete any files that may be held on the computer system or to monitor any internet sites visited. This statement serves to fulfil the school's obligations under the Data Protection Act.

· All computer activity should be appropriate to the level of ability and for their individual education progression. Use for private purposes is only allowed in exceptional circumstances and through consultation with the principal.

· Access must only be made via the authorised account and password.

· Pupils will be held responsible for any inappropriate use of the internet or email provision made through their usernames and passwords.

· The use of the internet and email is externally monitored by the system providers.

· Activity that threatens the integrity of the school ICT Systems or activity that attacks or corrupts other systems is forbidden.

Staff should read and sign a copy of the school's Acceptable Internet Use Agreement for Staff and return it to the ICT Coordinator (Refer to Appendix 2).

Rules for Pupil Use of the Internet

All pupils may be given the opportunity to access the internet in school as the internet is an excellent teaching tool in the classroom. It is also an excellent learning tool for pupils as it can help them enhance their own independent learning and research skills.

The internet and emailing facilities when provided are for pupils to conduct research and communicate with others. Pupils are responsible for good behaviour on the internet just as they are in the classroom.

Pupils should not use the internet to search for or send offensive emails, messages or information. Pupils are to use the internet under the direction of the class teacher.

Pupils and parents should read and sign Acceptable Use of the Internet Pupil Agreement (Refer to Appendix 1).

Use of Email

The C2k computer system is owned by the school and is made available to staff:

· Supervised email may be made available for specific subjects.

· School email facilities must not be used for private correspondence.

· Posting anonymous or offensive messages and forwarding chain letters is strictly forbidden.

· Sending or displaying offensive messages or pictures is forbidden.

· Using obscene language is forbidden.

· Harassing, insulting or attacking others is forbidden.

Activities not permitted whilst on the school computer/laptop:

· Damaging computers, computer systems or computer networks.

· Downloading music without permission.

· Using the username and password of another person without permission.

· Trespassing in other pupils' folders, work or files.

· Using Instant Messaging (IM) without permission and outside of a class lesson.

Sanctions

Breaking of the rules will result in a temporary or permanent ban of using the internet. When applicable, senior management and parents / guardians will be informed, and further consequences may be necessary.

Multimedia Technology

Thornfield House School is aware of the educational benefits that proper use of communication technology provides for pupils. We have at least three iPads in each classroom for pupils and teacher use. We are also very aware of the potential for personal harm, hurt and damage to individuals by the misuse and abuse of this technology. The school is therefore concerned with making the provision of multimedia technology safe to use for both pupils and members of staff.

Use of iPads

In school many of the pupils use iPads as an educational tool and this is seen as beneficial by teachers as it helps enhance the learning experience of the pupils.

Pupils are not permitted to use iPads for the following:

· To send inappropriate pictures to others.

· Send hurtful messages.

· Access social networking sites (Facebook, twitter etc.).

· Access the internet without permission.

· Use bad language.

· Take photos of pupils / staff without permission or direction from the teacher.

· Take videos of pupils / staff without permission or direction from the teacher.

Use of Social Networking Sites and Chat Rooms

With the changes C2K are making there is as possibility that pupils may have access to social networking sites in the future. The school will monitor this and will be dedicated to showing pupils how to use sites safely and responsibly when applicable in the curriculum.

However, as pupils have smart phones, tablets, computers etc. they will be able to access such sites from home.

When contacting other pupils on social networking sites pupils should not:

· Use hurtful language.

· Send harmful messages.

· Upload offensive photos.

· Upload personal information about other pupils.

Thornfield School is not responsible for pupils' Facebook accounts or other social networking sites and therefore parents are advised to monitor them closely and ensure that all children's accounts are private. It is important to note that it is against the law for children under the age of thirteen to have a Facebook, Instagram or TikTok account.

Keeping Safe Online

It is very important that everyone knows how to keep safe online. Teachers will plan to teach an e-safety lesson each term. Below are some guidelines that will help ensure pupils stay safe online (this list is not exhaustive):

· Never share personal details online. For example, don't give out your name, address, email or school name.

· Never give out passwords .

· Don't believe everything you read or see online.

· Don't open an email that is 'suspicious' or if it is from a stranger.

· Tell a teacher or another adult if you get an offensive email.

· Tell someone about anything you feel is harmful, hurtful or offensive or that gives you a 'funny feeling'.

· Make sure the images you put online are appropriate and suitable.

· Respect the privacy of others. Don't post pictures or videos on the internet without permission.

· Never speak to strangers or arrange to meet up with them.

· Always ask a teacher or another trusted person when you are in doubt about something.

Please note:

Pupils need to know how to cope or what to do if they come across inappropriate material or situations online. E-Safety will be discussed with pupils on an on-going and regular basis. This should be discussed with the pupils in an age appropriate way as a set of rules that will keep everyone safe when using technology in school.

Staff Guidelines on Multimedia Technology and Social Networking Sites

This policy is not only aimed at protecting pupils of Thornfield House School but also staff. Staff should follow the guidelines below:

Mobile Phones and Texting

· Staff should not use their mobile phones to phone or text pupils.

· Staff should not have a pupil's mobile phone number on their phone.

· Staff should use the school phone when contacting pupils (if necessary).

· Staff should **never** respond to informal social texts from pupils.

Social Networking Sites / Chat Rooms Email

· Staff **should not** communicate with pupils via social networking sites and chat rooms .

· Staff **should not** become 'friends' with pupils on social networking sites.

· Staff **should not** become 'friends' with parents of pupils on social networking sites.

· Staff **should never** use their personal email address to contact pupils.

· Staff should only email pupils for educational purposes using their C2K email address and the pupil's C2K email address.

· Staff should not use personal email accounts for school business.

· Staff should let the Principal know if pupils or parents send 'friend requests' to them.

· Staff should let the Principal know if pupils send social / inappropriate emails to them.

Further Staff Responsibilities with Internet and Electronic Communications

· Staff username and password should never be shared with pupils.

· Staff must always view and plan online activities to ensure the material is appropriate to age and ability.

· YouTube video clips should **never** be used if staff have not had the opportunity to watch the full video prior to the lesson. Staff should **never** assume the content is appropriate as titles can be misleading!

· C2K email accounts should only be used for **professional** purposes.

· Personal email accounts should not be used during school hours.

· Personal devices **should not** be used to take images or videos of pupils without prior permission from the Principal (exceptional circumstances only). Images / videos must always be removed from personal devices immediately after use (no exceptions).

· Staff must ensure that written permission is obtained from parents / guardians before images or videos of pupils are electronically published.

· Staff must **never** use pupils' full names anywhere on the school website.

· Staff must not use pupils' full names in association with photographs.

· Staff must not 'befriend' pupils or parents on social networking sites.

· Mobile phones and other electronic devices must be switched to 'silent' mode unless permission has been given by the Principal to leave the sound on.

Further Guidance

Staff and pupils should note that they are responsible for anything that is done using their user ID. They are responsible for all information and data placed on the log in, they are also responsible for any emails including attachments sent on their log in. Members of staff must ensure that no pupil is given access to a computer that they are logged on, unless being supervised in a one to one situation. This will mean that the pupil will not be able to access sites that may contain inappropriate material.

Staff should be aware that all Internet 'traffic' (including email) is monitored, recorded and tracked by the C2K system. In addition, staff should always ensure that any internet searches involving sites that have been granted enhanced access to should not be carried out when children can view them, i.e. on the computer's screen or on an interactive whiteboard. It is important for staff to ensure the use of sites such as YouTube should only take place after the content has been checked therefore ensuring that children are not exposed to inappropriate content.

E-Safety and Acceptable Use- Staff

All staff will be asked to read and sign the 'Acceptable Use of the Internet- Staff Agreement' (Appendix 2) which focuses on e-Safety responsibilities in accordance with the e-Safety policy. All staff are subject to the terms outlined in this policy. Failure to comply may lead to disciplinary action.

E-Safety and Acceptable Use- Pupils

Pupil's will read 'Acceptable Use of the Internet Pupil Agreement' (Appendix 1) with teachers and parents. This should be discussed in an age appropriate way as a set of rules that will keep everyone safe when using technology in school. Pupils and parents will sign the agreement and return it to school.

E-Safety and Acceptable Use- Parents

The e-Safety Policy will be published on the school's website and parents will be encouraged to read the document.

E-Safety Team

As e-safety is an important aspect of Child Protection / Safeguarding Children with the school therefore, the school's e-safety team, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the e-Safety coordinator and e-Safety team to keep abreast of current e-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), INEQE and Childnet. This team has the responsibility for leading and monitoring the implementation of e-Safety throughout the school.

Thornfield School's e-Safety Team consists of:

· Miss S Hutchinson (ICT Coordinator and e-Safety Coordinator)

· Mrs D Logan (Designated Teacher for Child Protection / Safeguarding Children)

· Mrs L Bruton (Designated Teacher for Pastoral Care)

Appendix 1:

Acceptable Use of the Internet- Pupil Agreement

Acceptable Use of the Internet- Pupil Agreement

Children should be taught from the outset that they are responsible for their use on the Internet in school and that they should use it in a safe, responsible and appropriate manner. The following guidelines are shared and discussed with the pupils in an age appropriate way. Teachers should continually teach and stress the importance of safe use of the internet. Thornfield House School provides access for pupils to computers and the internet to support teaching and learning the rules below are employed to help keep everyone safe.

· I will access the computer system with my login and password.

· I will not access other pupils' files unless instructed to do so and under supervision.

· I will use the school computers only for school work.

· I will not bring files into school (on removable drives / media or online) without permission and under supervision.

· I will not upload inappropriate material to my workspace or memory stick.

· I will use the internet responsibly.

· I will only email people I know or those approved by my teacher using my C2k email account.

· I will not open suspicious emails or emails from 'strangers'.

· The messages I send or information I upload will be polite, courteous and not hurtful to others.

· I will not open attachments or download files unless I have permission from my teacher.

· I will not give my home address, phone number, send photographs or video or give any other personal information that could be used to identify me, my family or my friends unless my teacher has given permission.

· If I receive a message or see anything that makes me 'uncomfortable', I will not respond to it. I will save it and show it to the teacher or another adult.

· I know and understand that the school may check my computer files and may monitor the websites I visit.

· I know that my online activity at all times should not upset or hurt other people and that I should never put myself at risk.

Signed by the Pupil: _____

Signed by the Parent / Guardian:_____

Date: _____

Appendix 2:

Acceptable Use of the Internet- Staff Agreement

Acceptable Use of the Internet- Staff Agreement

In line with Thornfield House School's 'E-safety and Acceptable Use Policy' I understand:

· I must not engage in any on-line activity that may compromise my professional responsibilities or bring the name of the school into disrepute;

· The school has the right to monitor my use of the school's ICT systems, email and other digital communications;

· I will not search for, access, upload, download any materials which are inappropriate /illegal such as child sexual abuse images pornography, racist, sectarian or offensive material;

· I must immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal and ICT coordinator;

· The use of school ICT systems for personal financial gain, gambling, political purposes or advertising is forbidden;

· I must not disclose my C2K username and password to anyone else, nor will I try to use anyone else's C2K username and password;

· I will not use the school systems to access social media sites and I will not make or accept friend requests to/from pupils or parents of pupils;

· I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of photographs/digital images;

· I must not access, copy, remove or otherwise alter any other user's files, without their express permission; any activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems is forbidden;

· When communicating electronically with others I should be professional, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;

· Posting anonymous messages and forwarding chain letters is forbidden;

· The need to be cautious when opening attachments to emails, due to the risk of the attachment containing viruses or other harmful programmes;

· Copyright of materials must be respected;

· That this Acceptable use of the Internet Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school;

· The school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the context of the school's ICT policy;

· I will only use my personal mobile ICT devices as agreed in the school's 'e-safety policy';

· I should immediately report any damage or faults involving equipment or software, however this may have happened;

· That if I have been granted enhanced Internet access to certain websites using the C2K system I must ensure that at all times no pupil has access to a computer on which I am logged on (unless under my supervision). When performing internet searches I must ensure that the computer is not displayed on an interactive board, as search engines are no longer controlled;

· 'YouTube' for example has a wide range of educational opportunities, however, I must always ensure that I have watched completely any videos I intend to use to ensure they are appropriate;

· When using C2K there is a log of my Internet searching history.

Staff Member: _____

Signed: _____

Date: _____