Thorn Grove Primary School

ACCEPTABLE USE POLICY

Introduction

The Internet provides access to vast amounts of information in the form of texts, images, sounds and video material. Through it, users may have access to libraries, websites, museums and government sites which may provide a rich and stimulating source of learning material.

The school will allow supervised access to the Internet for its pupils.

The Internet in School

We recognise that the Internet is a valuable resource that can enhance and enrich the learning opportunities for pupils and staff. However, the publication of material on the Internet is not currently rigorously controlled by any one regulatory body and it is therefore a source of **uncensored** information. This means that potentially, any child or adult user of the internet may encounter material that is inappropriate, distressing or misleading e.g. fraudulent, racist, pornographic, or over explicit in its nature.

At Thorn Grove, we are aware of these issues, but consider the advantages of using the Internet to outweigh the disadvantages. It is hoped that, as we educate our children in responsible and discriminating use of the Internet in school, this will set a standard and guidelines for its use in other contexts. Children may have access to the Internet both at home and within the community and at Thorn Grove we recognise that we work in partnership with parents and families, who also have a responsibility for educating children in this area.

We use the LEA (Local Education Authority) as our Internet Service Provider (ISP), and use their centralised filtering tools and firewalls to identify, block and restrict as much of the inappropriate material and content as is possible. The LEA has a stringent policy for internet security and safety, but unfortunately (as is the nature of the systems) no filtering tool has the ability to provide full comprehensive coverage and some content that may be deemed inappropriate may still be accessed. This is why the teaching and supervision of appropriate online use is vital in our setting.

The Internet and the use of online content in the Curriculum

Class teachers will be encouraged to use engaging materials from all sources, including the internet, and are responsible for carefully planning Internet usage into their teaching activities. It is essential that all online content be watched and interrogated fully prior to use and exposure to the pupils or other staff. It is also expected that appropriate records are kept in planning of suitable websites or sources of information.

Subject co-ordinators will be encouraged to find out suitable websites for their subject area, check content and pass this information on to other staff.

The Computing co-ordinator will be responsible for assisting staff to develop their own research skills including the effective, legal and safe use of information retrieved.

Website Safety

Children will be encouraged to explore websites that their teachers have identified as suitable sources for learning (see above guidance). The children will agree not to purposely attempt to access unsuitable or inappropriate content and will understand that sanctions will be given if this occurs.

The school has developed its own website. The Headteacher has had overall responsibility for the material published on this site and teachers will upload content from trusted sources and hardware. Parental permission will be obtained from parents before their child's photograph is published at the beginning of their time in school.

Children and adult users will be encouraged to check that all files are safe, secure and do not represent a threat to networks and security prior to downloading. The best practice in this case is to

check with the Computing Leader before any files from external sources are downloaded on to school computing hardware.

Managing Email and email safety

Each child, from Year 2 onwards, may be given the chance to have their own email address; if they are presented with this opportunity, they will be taught how to use email responsibly and safely in lessons. Children will be taught not to reveal any personal information, either their own or others, over the Internet. This includes, but is not exclusive to, names, addresses, phone numbers or agreeing to meet someone without parental consent.

Emails may carry attached files and documents. Potentially, these may carry viruses. The children will be taught not to open emails unless they know who has sent them and anti-virus software is installed.

Children will also inform supervising staff if they are uncomfortable about any messages or material they encounter when using the Internet. Staff will then inform the Computing Subject Leader who will arrange to have the site blocked, the email traced or report to other regulatory bodies if it is deemed appropriate. A record will be kept of any such incidents by the Computing Subject Leader.

Acceptable Use

All adults and children are expected to use the software and hardware systems linked with school in a responsible manner. It is not possible to set a fully comprehensive and specific rules about what is individually unacceptable but the following list provides guidelines on the appropriate use:

Etiquette and Privacy

All users are expected to abide by the rules of online etiquette. These rules include, but are not limited to, the following:

1. **Be polite** – never send or encourage others to send abusive messages
2. **Use appropriate language** – users should remember that they are representatives of the school on a global public system
3. **Do not engage in any action that may contravene any laws** - illegal activities of any kind are strictly forbidden.
3. **Monitor language** use - Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. **Ensure privacy of information** – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders. Use encrypted software and hardware to protect the data and information being used.
5. **Ensure Password Security**– do not reveal your password to anyone. If you think someone has obtained your password then contact the Computing Subject Leader.
6. **Understand School Electronic mail scrutiny** – School email is not guaranteed to be private. Messages relating to, or in support of, illegal activities will be reported to the authorities.
7. **Protect against disruption of work and use** – do not engage in any activities that would disrupt the use of the school systems by others.
8. **Do not access Social Media Sites on school devices**- Pupils and staff will not be allowed to access social media sites on school computing devices and adults may only access sites on personal devices in specific areas in school.
9. **Report Concerns** - Staff or students finding unsuitable content whilst using devices in school should report the details to the Computing Subject Leader as soon as possible.
10. **Protect the security of the School network** - Do not download files, introduce CD's or 'pen drives' into the network without having them thoroughly checked for viruses.
11. **Do not attempt to visit websites that night be considered inappropriate** - Such sites would include those relating to any illegal activity or contain content that may compromise the safety of the individuals involved. All online activity will be logged by the LEA network if not on the specific device and downloading material considered to be illegal may cause the police or other authorities to be called to investigate such use.

13. **Checking of files and software** – The Computing Subject Leader will regularly check the files and programmes stored on the school network for suitability.
14. **Responsibility for use** - It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet/Intranet does not occur.

Unacceptable Use

Examples of unacceptable use include, but are not limited to, the following:

- Purposely accessing, creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The LEA have filters in place restrict potentially risky content, but as discussed previously, these are not 'water-tight' and some accidental exposure to content may occur)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates the Data Protection Act or breaches the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- It is the responsibility of all users to fully comply with the acceptable use policy of any other networks or online areas that they access.
- Users must not download software without approval from the Computing Subject Leader.

Safeguarding:
All concerns about the welfare and safety of children and adults should be treated with the upmost urgency and the pathway for reporting these issues in the Safeguarding Policy should be followed and supersede any reporting to the Computing Subject Leader outlined above.

Mr G Wilson
Computing Lead
September 2017

Appendix A : Staff Code of Conduct for Computing and use of related equipment.

Staff Code of Conduct for all Computing related equipment (including visitors to the School)

The purpose of the code of conduct is to: provide guidance about safer working practice; help keep personal and private information separate; keep adults and children safe when using electronic media; and adopt responsible behaviour that should prevent staff putting themselves and their career at risk.

This document refers to professional working relationships with colleagues, children, young people, parents /carers, other adults and volunteers.

As a member of staff at Thorn Grove Primary School I will not:

- Give personal details or information to children/young people. This includes mobile phone numbers, details of blogs, details of personal websites, social networking accounts, passwords, PIN numbers and log-in details
- Give my passwords and Log In details to anyone
- Use my personal mobile phone to communicate with children/young people except in genuine emergencies and
- Make available personal details or information on a social network site with children/young people. It is important to be aware that applying appropriate privacy settings and carefully selecting group membership is a responsible action that can assist good practice in this specific area
- Add/allow a child/young person to join my contacts/friends list
- Use the internet or web-based communication to send messages to children/young people unless it is part of a controlled supervised in-school activity.
- Use my personal e-mail address in any communication with children and young people
- Tick the 'remember me' box when using password protected internet sites in school
- Retain pupil/family contact details for personal use (dispose of these securely and swiftly after use)
- Produce, store or retain images of children and young people on any personal device, or for personal use.
- Only produce or store images of children and young people if appropriate permission has been sought
- Use school information systems for private purposes without the permission of the Headteacher or designated alternate
- Install any additional hardware or software without the permission of the Headteacher or designated alternate
- Upload or download inappropriate or illegal material, nor assist children, young people and other adults in this process

I Will:

- Only use my mobile phone in line with school policy during directed time.
- In the extreme cases where I have no other choice but to use my mobile phone to contact parents, carers and volunteers, anonymise my mobile phone number (best practice is to use a school mobile phone or official and secure email accounts)
- Switch off any blue tooth visibility in around school and at school events
- Use passwords to protect, switch off and lock my technology when it is not in use
- Ensure that all written communications are compatible with my professional role
- Remember that on-line conversations are written documents and should be treated as such
- Store images of children/young people in the secure network space specified by the school and only use school equipment and devices to take pictures.
- not use a personal camera or a mobile phone to take pictures of children or young people

- Remove any contact details of children/young people /parents/carers/volunteers from a mobile device once the activity is complete. This includes school equipment and my personal mobile if permission for its use has been granted
- Respect copyright and intellectual property rights
- Ensure that a recognised and up-to-date anti-virus product is operating on any computer used when working through the Remote Access portal (Authorised by the School and LA)
- Ensure that any personal device used to work remotely is protected by a firewall at all times when it is connected to the internet.
- Ensure that the a robust and secure password (in accordance with the LA guidance) be used when working remotely

I will consult the Headteacher if:

- I have an existing social relationship with a child/young person/parent/carer / volunteer outside school which leads me to communicate with them using technology
- I have an existing social relationship with a child/young person/parent/carer/ volunteer outside school which leads me to play on-line games with them

I understand the advice listed below:

Thorn Grove Primary School recommends that you:

- Set your privacy settings at a maximum for any social network site/image storage site etc.
- Make sure that any personal information that is publicly available is accurate and appropriate to your professional role
- Are mindful about how you present yourself when you are publishing information about yourself, accessing content or having interacting with others on-line
- Assume that **any** information that you post is publicly available

Additional Requirements:

Please tick

- ☐ I am aware that I must not behave in a way that could suggest that I am trying to develop a personal relationship with a child known to me through my professional role
- ☐ I have read the E-Safety Safer Working Practice Guidelines produced by Stockport Safeguarding Children Board
- ☐ I will report any incidents and concerns of a breach of E-safety regarding children/young people to the Designated Safeguarding Lead in school
- ☐ I am aware that some activities I undertake within my private life, using technology, may have the potential to bring the profession/establishment into disrepute
- ☐ I understand that the Headteacher may ask to view my school equipment at any time
- ☐ I have read and understand the above Code of Conduct

Signed: Full Name: Date:	Received By: Role: Date: *Original copy to be stored in school personnel file* *Copy to be retained by member of staff*

Appendix B : Key Stage 1&2 Parents letter

Dear Parents and Carers,

We have been discussing online safety at school and we would like to give the children the opportunity to discuss the advice we have been talking about with adults and older siblings at home. Hopefully explaining how the actions we use in school can be a benefit to those outside school.

As a school we consider the online environment to be a valuable learning resource, but understand the potential risks that may present themselves to young people when using the online environment.

Today, in assembly we reminded children about these key messages:

Images used coutesy of CEOP and Thinkyouknow

Zip it- Keep your personal information private and think about what you say and do online
Block it- Block people who send you nasty messages and don't open unknown links and attachments
Flag it- Flag up with someone you trust if anything upsets you or if someone asks to meet you offline
THINK – Remember the five statements when posting or communication online.

We publish important information on our website to support e-safety at the following address: http://www.thorngroveprimary.co.uk/online-safety-2/

As part of our programme of events we would like the children to create a poster (no larger than A3), that can be displayed in the classrooms and corridors of school, that spreads the message and promotes safe online use.

All posters must contain the three key messages above and can be created by children on their own or with the help of adults.

We will publish the winning entries on the website and will be giving prizes for the best poster in each class, key stage and an overall prize for the whole school.

The entries will be judged by the school council and a selection of staff. The judging criteria is below:

1. Does the poster clearly state and explain the main action points 'Zip It, Block It' 'Flag It' and 'THINK'?
2. Is the poster vibrant and eye- catching?
3. Does the poster show a new and interesting way of promoting the message?

The closing date for entries is: Friday 8th December.

If you have any questions about enjoying the online environment in a safe and responsible way, please contact me at school.

Yours Sincerely

Mr Wilson
Deputy Headteacher and Computing Lead

E-Safety Rules

These E-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school computing systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposed is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.