Thomas Gainsborough School
Online Safety Policy

Policy Ratified: April 2017
Policy Review: April 2019

Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of Thomas Gainsborough School (TGS) to ensure that children and young people are protected from potential harm both within and beyond the school. This is also set out in the government's Keeping Children Safe in Education, 2016 document. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

This policy should be read in conjunction with the school's Safeguarding Policy and Behaviour Policy.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff and students about the pros and cons of using new technologies both within and outside the school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

1: Roles and Responsibilities of the school.

1.1 Governors and Head teacher.

It is the overall responsibility of the Head teacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Head teacher has a designated Online Safety Lead and Safeguarding Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the school

- The Head teacher is responsible for promoting online Safety across the curriculum and has an awareness of how this is being developed and implemented.

- The Governors MUST ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.

- The Safeguarding Governor challenges the school about having appropriate strategies which define the roles and responsibilities for the management, implementation and safety for using ICT, including:
    - Firewalls
    - Anti-virus and anti-spyware software
    - Filters
    - Using an accredited ISP (Internet Service Provider)
    - Awareness of wireless technology issues
    - A clear policy on using personal devices

  And that any misuse or incident has been dealt with appropriately according to policy.

1.2: Local online safety Lead

It is the role of the designated online safety lead and safeguarding lead to:

- Appreciate the importance of online safety within the school and recognise that all educational establishments have a general duty of care to ensure the safety of their students and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that up-to-date information and that training is available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and students, in the initial set up of a network, stand-alone PC, staff/student laptops and the school learning platform.
- Ensure that all adults are aware of the filtering levels and why they are there to protect students.
- Report issues and update the Head teacher.
- Liaise with the relevant staff to ensure that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure form the SSCB to ensure the correct procedures are used with incidents of misuse.
- Work alongside the ICT team and network manager to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails and report to the Head teacher any concerns.

1.3: Staff or Adults

It is the responsibility of all adults within the school to:

- Ensure that they know who the Designated Safeguarding Lead (DSL) for Safeguarding is within the school so that any misuse or incidents can be reported which involve a student.
- Where an allegation is made against a member of staff it should be reported immediately to the Head teacher/DSL. In the event of an allegation made against the Head teacher, the Chair of Governors should be informed immediately.
- Be familiar with the Behaviour, Bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately.
- Alert the DSL of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that students are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Students should know what to do in the event of an incident.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the DSL and the IT helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed 'bullying' or other inappropriate behaviour via the Internet or other technologies to the DSL or Head teacher.

1.4: Students

Students should be:

- Responsible for following the Acceptable Use Agreement whilst within the school as agreed at the beginning of each academic year or whenever a new student attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE, assemblies and throughout the curriculum, when appropriate.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.

2: Appropriate and Inappropriate Use

2.1: By Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service ad know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Head teacher/DSL immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and al appropriate authorities contacted.

2.2: By Students

Acceptable Use Agreements are in student planners. The agreements are there for students to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions.

The school should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreements are accepted by the student with the support of the parent/carer.

Should a child or young person be found to misuse the online facilities whilst at the school, the incident will be investigated and students will be punished in accordance with our Behaviour policy and parents will be informed.

A serious infringement could result in isolation, fixed term exclusion or a permanent exclusion dependent on the severity of the offence. The police may also be informed and a safeguarding referral may be made.

2.3: Internet Use

The school teaches students how to use the internet safely and responsibly. They are also taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning.

These skills and competencies are taught within the curriculum so that students have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Students should know how to deal with any incidents with confidence.

2.4: Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners ad recognise the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

2.5: Learning Platforms

The uploading of images to the school website is subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of

any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

2.6:E-mail Use

The school has e-mail addresses for students to use as individuals as part of their entitlement to being able to understand differ ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse.

Staff and students use their school email address for any communication between home and the school only. A breach of this may be considered a misuse.

Teachers are expected to monitor their class use of emails where there are communications between home and the school on a regular basis. The network manager regularly monitors internet use and the use of emails. The network manager notifies the Head teacher/ DSL of any infringements.

2.7: Personal Mobile Devices – Students

Students must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras

Students should be aware that games consoles such as Sony PlayStation, Microsoft Xbox, Nintendo Wii and other such systems have Internet access which may not include filtering and should not be used in the school.

Thomas Gainsborough School is not responsible for any theft, loss or damage of any personal mobile device.

2.8: Personal Mobile Devices – Staff

Staff must not use personal numbers to contact students under any circumstances.

Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras

3: School Devices

The school must ensure that students understand the use of a public domain and the consequences of misuse. Relevant curriculum links are made to highlight the legal implications and the involvement of law enforcement. Other technologies which the school use include:

- Photocopiers
- Fax machines
- Telephones
- Mobile phones
- Cameras
- Video recorders
- Voice recorders
- Tablets

3.1: Videos and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in the school there is access to cameras, video recorders and voice recorders, this should be monitored by members of staff. Students therefore should not have, nor be using, such equipment without the express permission of a member of staff.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

3.2: Managing Social Networking and Other Web 2.0 Technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private place through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and students are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Twitter and Snap chat)

In response to this issue the following measures should be put in place:

- The school controls access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school uniform).
- Students are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the Behaviour Policy, to be followed.

3.3: Social Networking Advice for Staff

Social networking outside of work hours, on non-school equipment, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking in conjunction with the training given in their Safeguarding training.

- Personal details are never shared with students such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of authorised systems (e.g. email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a professional level. As such, professional communications using school e-mails and the VLE are permitted. Any abuse of this system should be reported to the relevant member of staff (line manager, any member of SLT or Head teacher).

4: Safeguarding Measures - Filtering

The school is responsible for setting its filtering systems. It is the responsibility of the Governing Body and the Head teacher to ensure that the filtering systems protect young people from inappropriate materials.

The levels listed below are in relation to age appropriate categories:

- Staff- Basic adult policy. This allows for some customisation and the addition of sites if agreed by the IT Network Manager
- Students – Basic student policy. All sites are blocked except for accepted sites provided by staff, checked by the IT Manager and that conform to safe search protocols.
- Internet search engines are forced through 'safe search' as a matter of course, as are 'You Tube' and similar products.

Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about people and the school cannot be accessed by unauthorised users.

Links or feeds to online safety websites are provided.

The Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for students to report an incident if they feel they cannot talk to a known adult.

5: Curriculum Development

The teaching and learning of online safety is embedded within the school's curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line. It is delivered on a regular basis through a variety of means such as ICT lessons, assemblies and Theme of the Fortnight.

Key Staff:

Helen Yapp – DSL
Emma Wilson Downes – Online Safety Lead
Stuart Bloyce – Network Manager
Jenny Smith - Governor