National Teaching School
designated by
National College for
Teaching & Leadership

Tapton SCHOOL

Ofsted Outstanding School 2012|2013

Executive Headteacher: Mr David Dennis
Tapton School Academy Trust, Darwin Lane, Sheffield, S10 5RG Tel: 0114 267 1414 Fax: 0114 294 1155
Email: enquiries@taptonschool.co.uk Web: www.taptonschool.co.uk Twitter: @Taptonschool1

Tapton School

E-Safety Policy

September 2016

AUTHOR: Steve Rippin

COMMITTEE: Learning and Inclusion

LAST REVIEW/UPDATE: September 2016

LEVEL OF CHANGE: Minor

NEXT REVIEW: June 2017

Contents

Overview

This e-safety policy was created through consultation with a number of stakeholders in Tapton School consisting of:

David Dennis (Co-Headteacher)
Steve Rippin (Assistant Headteacher)
Liz Drayton (ICT strategy Manager)
Kath Tabani (Behaviour & Safety Manager and Child Protection Liaison Officer)
Debra Kirkham (Business Manager)
Naeem Al-Alawi (Subject Leader for ICT)
Hayley Sharman (Subject Leader for PSHEE)

Any questions, queries or concerns relating to this policy or any e-safety issues in general should be discussed with a member of the **e-safety Management Group** which consists of **David Dennis**, Headteacher, **Liz Drayton**, ICT Strategy Manager and **Steve Rippin**, Assistant Headteacher.

Introduction

Tapton School recognises the immense benefits that ICT, internet, Learning Platform and a wide range of electronic communication provide for the development of high quality learning experiences across our school community.

We wish to actively promote engagement in the range of technologies available throughout our whole school community. With the advent of student and parental engagement through our Learning Platform, a whole new level of communication and active engagement is available to us which enables us to operate within a wholly transparent and cohesive learning environment.

Tapton School also recognises the need to balance the benefits of these technologies with a thorough awareness of the potential risks. It is vital that our whole school community understands and adheres to the e-safety policy that ensures safe, appropriate and responsible use of such technologies. This policy is designed to reflect our commitment to the safeguarding and well being of our students.

Responsibilities of the Tapton School Community

We believe that e-safety is the responsibility of the whole school community and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Management Team

- Develop and promote an e-safety culture within the school community.
- Support the e-safety Management Group in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to e-safety effectively.
- Receive and regularly review e-safety incident logs and be aware of the procedure to be followed should an e-safety incident occur in school.
- Take ultimate responsibility for the e-safety of the school community.

Responsibilities of the e-safety Management Group

- Promote an awareness and commitment to e-safety throughout the school.
- Be the first point of contact in school on all e-safety matters.
- Lead the school e-safety group.
- Create and maintain e-safety policies and procedures.
- Develop an understanding of current e-safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in e-safety issues
- Ensure that e-safety education is embedded across the curriculum.
- Ensure that e-safety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on e-safety issues to the e-safety group and SLT as appropriate
- Ensure an e-safety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff including VS resource

Read, understand and help promote the school's e-safety policies and guidance.
Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
Develop and maintain an awareness of current e-safety issues and guidance.
Model safe and responsible behaviours in your own use of technology.
Embed e-safety messages in learning activities where appropriate.
Supervise students carefully when engaged in learning activities involving technology.
Be aware of what to do if an e-safety incident occurs.
Maintain a professional level of conduct in their personal use of technology at all times.

Please note that any visitors to school who may be shadowing or supporting a department must only access the school network under supervision of a member of staff.

Responsibilities of Technical Staff

Read, understand, contribute to and help promote the school's e-safety policies and guidance.
Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
Support the school in providing a safe technical infrastructure to support learning and teaching.
Take responsibility for the security of the school ICT system.
Report any e-safety related issues that come to your attention to a member of the e-safety Management Group.
Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to your work.
Liaise with the local authority and others on technical issues.
Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Students

Read, understand and adhere to the school student Acceptable Use Policy (AUP).
Help and support the school in creating e-safety policies and practices and adhere to any policies and practices the school creates.
Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know someone who this is happening to.
Discuss e-safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

Help and support your school in promoting e-safety.
Read, understand and promote the school student AUP with your children.
Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
Discuss e-safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
Model safe and responsible behaviours in your own use of technology.
Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

Read, understand, contribute to and help promote the school's e-safety policies and guidance.
Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
Ensure appropriate funding and resources are available for the school to implement their e-safety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.

We will provide a series of specific e-safety related lessons in every year group as part of the ICT and PSHEE curriculum.
We will celebrate and promote e-safety through planned assemblies.
We will discuss, remind or raise relevant e-safety messages with students routinely wherever suitable opportunities arise during all lessons; 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.
We will remind students about their responsibilities through an end-user AUP which every student will sign. The student AUP will be displayed throughout the school and displayed when a student logs on.
Staff will model safe and responsible behaviour in their own use of technology during lessons.

How Parents and Carers Will Be Involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on e-safety regularly on our school website, parent site of the Learning Platform and through our school newsletter (Tapton Update) and student planners
- Consult parents through parental survey either through the Learning Platform or in paper form if requested.

Managing ICT Systems and Access

Tapton School, in partnership with our technology providers, will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

Servers, workstations and other hardware and software will be kept updated as appropriate.

Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.

The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

All users will sign an end-user Acceptable Use Policy (AUP) provided by the school. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.

All Tapton students will access the Internet using an individual log-on, which they will keep secure.

Whether supervised by a member of staff or working independently, students will abide by the school AUP at all times.

Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.

The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet Access

The school uses a filtered Internet service. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform a member of the e-safety Management Group.

If users discover a website with potentially illegal content, this should be reported immediately to a member of the e-safety Management Group. The school will report this to appropriate agencies including the filtering provider.

The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning Technologies In School

Our policy on staff and student use of a range of learning technologies is summarised in the following table. Staff and students should also refer to the Acceptable Use Policy whenever engaging with such technologies.

	Students	**Staff**
Personal mobile phones brought into school	Students allowed for use outside of school building and in designated areas only	Staff allowed in appropriate places at appropriate times
Mobile phones used in lessons	Students allowed with permission as part of a learning activity	Staff not allowed unless exceptional permission given by member of SLT
Mobile phones used outside of lessons	Students not allowed inside the school building except in designated areas	Staff allowed in appropriate places at appropriate times
Taking photographs or videos on personal equipment	Students allowed with permission as part of a learning activity but must never be shared outside of Tapton School	Staff should use school devices except, in exceptional circumstances, for identification purposes, ensuring footage will never leave school premises.
Taking photographs or videos on school devices	Students allowed with permission as part of a learning activity	Staff allowed as part of a school based activity providing data is not taken off site
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Students allowed with permission as part of a	Staff allowed during designated breaks

	learning activity or during designated break times	
Use of personal email addresses in school	Students not allowed	Staff allowed but not for school business
Use of school email address for personal correspondence	Students allowed	Staff allowed
Use of online chat rooms	Students not allowed	Staff not allowed
Use of instant messaging services	Students not allowed	Staff allowed during designated breaks in appropriate places
Use of blogs, wikis, podcasts or social networking sites	Students allowed with permission as part of a learning activity through the Tapton Learning Platform	Staff allowed as part of a school based activity through the Tapton Learning Platform

Using email

Staff and students should use approved email accounts allocated to them by the school, and be aware that their use of the school email system will be monitored and checked.

Students will be allocated an individual email account for their use in school.

Students will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening email from an unknown sender, or viewing/opening attachments.

Communication between staff and students or members of the wider school community should be professional and related to school matters only.

Any inappropriate use of the school email system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

We will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Digital images, video and sound will only be created using equipment provided by the school or on personal equipment under the supervision of a member of staff.

Staff and students will follow the school policy on creating, using and storing digital resources. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full

names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/students involved.

If students are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, social networking and other ways for students to publish content online

Blogging, podcasting and other publishing of online content by students will take place within the school learning platform. Students will not be allowed to post or create content on sites where members of the public have access.

Students will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them. Students will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.

Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using mobile phones

Personal mobile phones will only be used during lessons with permission from the teacher. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone should be provided and used. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a student or parent.

Using new technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-safety point of view.

We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-safety risk.

Protecting Personal Data

We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff will ensure they properly log-off from a computer terminal after accessing personal data.

Staff will not remove personal or sensitive data from the school premises without permission of the Co-Headteacher, and without ensuring such data is kept secure. Data taken off site should be encrypted via a portable device such as a USB.

Staff must ensure that their access to Sims takes place in a secure environment and should never leave Sims open if unattended. Staff should be particularly vigilant if Sims is open during a lesson and ensure that students are not able to access sensitive data.

When downloading or transferring data to the MLE department site or specific class site staff must ensure such data is not transferred to the student site of the MLE where students would have access to potentially sensitive data.

The Tapton School Website and Other Online Content Published by the School

The school website will not include the personal details, including individual email addresses or full names, of staff or students.

A generic contact email address will be used for all enquiries received through the school website.

All content included on the school website will be approved by a member of the safety Management Group before publication.

The content of the website will be composed in such a way that individual students cannot be clearly identified.

Staff and students should not post school-related content on any external website without seeking permission first.

Dealing With E-Safety Incidents

It is vital that all members of our school community are fully aware of the potential incidents that may arise from improper use of technologies, the importance of being constantly vigilant in the monitoring and reporting of any such incidents and that improper and inappropriate use of technologies will result in a staged approach to sanctions including the removal of internet permissions for a fixed period of time, in addition to the full range of other behaviour sanctions in line with the School behaviour Policy. Staff are reminded that improper and inappropriate use of technologies in school may result in disciplinary or criminal action depending on the severity of the offence.

Potential breaches of protocol which must be avoided

E-Safety incident	Potential user
Accessing illegal content deliberately	Students and Staff
Accessing inappropriate content deliberately	Students and Staff
Accessing illegal content accidentally and failing to report this	Students and Staff
Accessing inappropriate content accidentally and failing to report this	Students and Staff
Inappropriate use of personal technologies (e.g. mobile phones) at school	Students and Staff
Accessing social networking sites, chat sites, instant messaging accounts or personal emails where not allowed	Students and Staff
Accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time	Students and Staff
Downloading or uploading files where not allowed	Students and Staff
Sharing your username and password with others	Students and Staff
Accessing school ICT systems with someone else's username and password	Students and Staff
Opening, altering, deleting or otherwise accessing files or data belonging to someone else	Students and Staff
Using school or personal equipment to send a message or create content that is offensive or bullying in nature	Students and Staff

Attempting to circumvent school filtering, monitoring or other security systems	Students and Staff
Sending messages or creating content that could bring the school in to disrepute	Students and Staff
Revealing the personal information (including digital images, video or text) of others by electronic means (e.g. sending of messages, creating online content) without permission	Students and Staff
Use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)	Students and Staff
Transferring personal data insecurely	Staff
Using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones or communicating via social networking sites)	Staff
Failure to abide by copyright of licensing agreements (for instance, using online resources in lessons where permission is not given)	Staff

Tapton School - Student Acceptable Use Policy

Here at Tapton School we want every student to embrace the use of ICT, internet and a wide range of electronic communication to enhance learning. However, it is vital that every student fully understands and adheres to the required policy that ensures safe, appropriate and responsible use of such technologies. The agreement set out on this page applies to any activity undertaken both in school and outside of school. Misuse of the ICT system, internet or any form of electronic communication will result in you being denied use of this provision as well as further sanctions. Please take time to read this agreement carefully and make sure you fully understand each point before signing the agreement.

- I will only access the school ICT system and Internet via my authorised account and password, which I will not make available to others.
- I will ensure that I do not willfully damage the system by means of malicious code (e.g. virus infections, malware etc), hacking or physical tampering.
- I will ensure any portable devices such as USB sticks do not contain malicious software before downloading any files on to the school network.
- I will not play computer games during the school day unless I have been directed to do so and they support my learning.
- I will not willfully interfere with and/or delete another person's work files.
- I will not use chat rooms and social networking sites during the school day.
- I will not send or forward messages, publish or create material which is offensive, hurtful or otherwise upsetting to another person. Nor will I post anonymous messages or forward chain letters.
- Language which I use in electronic communication will be appropriate and suitable as for all school work.
- I will not use mobile phones, cameras or other electronic devices to take, publish or circulate pictures or videos of anyone without their permission.
- I will respect copyright of all materials, will avoid plagiarism (copying of someone else's work) when using ICT or internet to produce school work.
- I understand that the use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden and may constitute a criminal offence.
- Guidelines for safe use of the internet will be followed at all times and I will report any materials or conduct which I feel is unacceptable.

I have read and understood the above statements and I agree to comply with Tapton school rules for use of ICT facilities and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Student signature.....Form Group.....

Student full name.....Date.....

Tapton School – Staff Acceptable Use for E-Safety Policy

Tapton School recognises that the use of ICT, internet, MLE and a wide range of electronic communication can greatly enhance the quality of learning across our school community. It is vital that every member of staff fully understands and adheres to the required policy that ensures safe, appropriate and responsible use of such technologies. Please take time to read this agreement carefully and make sure you fully understand each point before signing the agreement.

- I will keep my login, email address and password confidential. I will take care to ensure that others cannot use my accounts to access confidential information about students or staff by always logging off when I have finished work or locking my computer when it is left unattended.
- I will never use anyone else's login, email address or password or access their work without their permission.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for students and their parents.
- Any form of electronic communication with students or parents will only be via the school's accredited system or Learning Platform.
- I will ensure that all communication, including communication via social networking sites (eg, Face book) is transparent and open to scrutiny.
- I will ensure that communication between myself and students, by whatever method, should take place with clear and explicit professional boundaries. "Think before you Post!"
- I understand that the use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded and notify my line manager if I suspect someone else of misusing ICT facilities or the internet.
- I understand that I must also inform the designated Child Protection Liaison Officer if misuse may be a child protection issue.
- I will ensure that students under my supervision use ICT facilities and the internet appropriately to support learning. I will challenge and report any misuse.
- I will screen all USB pens, digital media and portable devices for malicious software before I download any files to the network and take care when opening unknown email attachments. I will seek advice from the ICT strategy manager if I am unsure about the safety of any such devices or attachments.
- I will not attach any devices to the network which may contain files which breach copyright, data protection or other laws.
- I agree to use the school's ICT facilities and internet only for work related use during my working hours (excluding designated breaks).

- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will only use my mobile phone during non-teaching time. It will be turned off or kept on silent mode during lessons except in an emergency situation with the agreement of a member of the Senior Leadership Team.
- I will only use my mobile phone or other electronic equipment to photograph or video students as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage never leaves school premises.
- I understand that the school reserves the right to check files and monitor the internet sites used by staff.
- I understand that the misuse of ICT facilities and the internet could result in disciplinary action being taken against me.

Staff member's signature.....

Staff member's full name.....

Date.....