Social Media and e-Safety Policy

Written by: Jonathan Hobbs and Anja Toddington **Date:** January 2017
Approved by: DSL **Date:** May 2017
Reviewed by: Gaby Wood **Date:** January 2018
Date for next review: Sept 2019

Policy Statement:

We now live in an age when many of us use the internet on a regular basis. This tool, like any tool, can be used in a healthy and safe way, or an unhealthy and dangerous way, especially if you use it without knowing how to. Most mobile devices provide internet access such as desktops, laptops, phones, iPods, tablets, kindles, etc. With so many devices now in all of our homes, the guidance below hopes to inform and guide about how keep children safe when using the internet and Social Media.

As a school we aim to safeguard the wellbeing of our students and our members of staff. As such, we wish to set appropriate boundaries for the out of school relationship, being particular mindful of online contact between students and staff.

What are the risks?

There can be seen to be three main areas of risk from the internet:

1. Inappropriate contact from people.
2. Inappropriate content found or seen.
3. Private information being unwittingly shared.

Inappropriate contact from people

The internet can be used to connect people, making working or socialising with others in different places possible when previously it was not. It also allows us to share our thoughts and interests with our friends. Although this can be positive, there are those who choose to exploit this openness. There are some who assume false identities to get to know unwary and unsuspecting victims. Watch this video to find out more: *Sam's Real Friends: www.youtube.com/watch?v=tBmW7OlQLdI*

To help protect against this be a T.E.A.M

Talk to your child/ren
regularly about websites, apps and other digital services they enjoy using and encourage them to tell you if they are concerned about anything they see online. Make sure your child is only 'friends' with people they actually know. This is a good way to help your child learn to navigate the net; talk to them about their use and learn how to use it competently yourself. If you are able to talk to them openly about what they are doing, or what you are doing on the internet, they can learn that you are holding consciousness around this topic, that you are informed and interested in what they are doing and how they are using it. If you are also able to learn how to use it yourself, you will be better placed to educate and guide them as they are initially learning, whilst knowing they are doing so within the boundaries you feel appropriate.

Explore their online world together

Agree boundaries
and rules about what is ok and what's not such as making personal contact details (phone number, address, birthdate etc.) available online.

Manage your family's settings & parental controls set to private on all online accounts.

- Brook's online tools section: www.brook.org.uk/your-life/category/staying-safe-online
- Internet Matters: www.internetmatters.org/parental-controls/
- Childnet: www.childnet.com/parents-and-carers/hot-topics/parental-controls
- NSPCC: www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
  Talk to someone on 0808 800 5002 (free O2 & NSPCC helpline about parental controls, privacy settings, advice on social networks, etc.

Think about your '**Digital Footprint'**

Digital footprints are the tracks we all leave online and are made up of the information we share about ourselves. This is important to be aware of because once you've shared something online, you have no control of it, you can't remove it or get it back and it will be there forever.

Try Googling your own name. Think carefully about what comes up and what the results say about you. Now put yourself in the shoes of your family, your teachers, lecturers or a potential employer. Many of us are guilty of making judgements based on what we see online about other people.

Inappropriate content found or seen

When children begin to use the internet, they will search for things of interest to them, either for school work, or for their own entertainment. Some of the content they can find you, as the parent, will be happy with, but there will be other content you would not want them to see. However, there are other ways that your child might meet content you are not happy for them to see, such as picture messaging on their phones.

Be aware of 8 types of websites

1. Pornography – distorted view of sex and relationships
2. Violent content
3. Illegal content - child sexual abuse, racist material, criminally obscene adult content
4. Misleading & harmful information – extreme political views, encourage harmful behaviour
5. Music, games, films & TV – legality and cost
6. Gambling – illegal for under 18's
7. Spam & scams – malware and trickery leading to grooming, identity theft, money scams etc.
8. Advertising – difference between editorial and advertising

Content through the internet

This could be accessed through a computer, laptop, phone, tablet, small handheld devices, games consoles, some televisions, and some satellite or freeview boxes. You can help to control what they see in the following ways:

- Have the family computer in a shared space, so you can see what they are looking at.
- Allow access to the internet only through this shared computer, not through mobiles, ipods, tablets or laptops.
- Restrict the content available by using the parental controls. You can access these through your internet provider. The following links may be helpful:
    - Mobile phone parental controls
      http://consumers.ofcom.org.uk/internet/online-safety-and-security/parental-controls-for-mobile-phones/
    - Internet provider parental controls
      http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

Content through mobile phones

Aside from the internet, mobile phones can also be used to share content which you feel is unsuitable for your child, such as indecent images. This is called Sexting, and you can find out more by visiting the Child Line Website shown below.

http://www.childline.org.uk/Explore/OnlineSafety/Pages/Sexting.aspx

Private information being unwittingly shared

When using social networking sites such as Facebook, Twitter, Snapchat, Instagram, Bebo, etc., the account holder provides information about themselves. The amount given is up to the user, but often the user is not aware how to hide this information, or even that this information is shared openly. Unless you ask for the information to be hidden, it will likely be public. You can test this by searching for yourself by using a search engine, and seeing what you can see of your profile.

When children start to use social networking sites, they are unlikely to be aware of this. To help keep them safe, create the account with them, show them how to adjust their privacy settings and connect with them through your own account if you have one. If they are unaware of their settings, anyone can find out their personal information, see their images and watch their activity. Below is another video which you may find useful for yourself, or to share with your children once they reach 12/13 years. Please put into YouTube search: *Internet Safety - Newsround Caught In The Web (9 Feb 2010)*

Student contact:

- Members of staff and students enrolled at South Devon Steiner School are required not to contact each other directly, through online mediums or using personal mobile phones, with the exceptions stated below in the **Exceptions** section.
- The school expects there to be **no contact** between a member of staff and a student via any of the following mediums:
    - Social networking sites including Facebook, Instagram, Snapchat, Myspace, Bebo, Twitter or similar
    - Email contact, unless otherwise agreed with either a member of the Safeguarding Group, Class Teacher or Class Sponsor and the student's parent.
        - If email contact does happen, a second member of staff is copied into the email and only school email addresses are used.
    - No contact through personal mobile phones.
        - There may be exceptional circumstances where this is necessary, such as during a school trip, but teachers should always use school mobile phones.
- Once a student has left the school, they and a member of staff may wish to communicate with each other through online mediums, such as email or Facebook. The school recognises that lasting and meaningful friendships will arise out of the work we enter into during our time at school together. As such, once a student has left South Devon Steiner School, the restriction on online contact will be lifted and members of staff and students are free to enter into out of school contact with each other.

Upper School

- There may be the need for teachers to engage in email contact with Upper School students, and may elect to use email for the distribution of work or study material. In this case, the following controls will be in place:
    - Teachers and students will only communicate about school work related matters.
    - The teacher will only use their school email address to communicate with students.
    - The teacher acknowledges that they may be asked to share the content of any email sent from their school account to a student or group of students.
    - The parent community will be aware that this contact is happening.

Safeguarding

- There may arise a situation where the student wishes to discuss personal information with a member of staff, and that they elect to use email. In this instance, their parents may not be informed of the contact via email. The following controls will be in place:
    - The student is willing to engage via email.
    - The member of staff is willing to engage via email.
    - The Safeguarding group is informed about this contact.
    - The member of staff will clearly state to the student who is aware of the content of the emails with the Welfare group.
    - The email contact happens using the member of staff's email account.
    - The student is aware that the school email may be seen by others.
    - The student is encouraged to meet face-to-face if possible.
    - The student's parents will be informed if necessary, and the student is aware of this as a possibility.

Controls:

- If a member of staff needs to contact a student, they will do so via the student's parent or legal guardian.
- If a student needs to contact a member of staff, they will do so during normal school hours, at school.
- The school trusts that members of staff will adhere to these outlines.
- The school will share this policy with our communities, explain the need for it, and ask for tolerance, understanding and help in keeping these boundaries clear.

Information/advice/guidance:

Useful Links and references

NSPCC - National Society for Prevention of Cruelty to Children website
Address: www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/
What will I find there?

- A guide to Social Media your child might be using.
- Advice as to how to engage in a conversation with your child around online presence and safety.
- Advice targeting specific concerns you might have around you child's use of the Internet.

Child Net
Address: www.childnet.com/parents-and-carers/
What will I find there?

- Information about online safety
- A hot topics section which explains and offer support with different usage of the Internet (apps, downloading, parental controls, gaming but also more sensitive topics such as cyberbullying or sexting…)

Internet Safety – type: "Newsround Caught In the Web" into You Tube or follow link
Address: www.youtube.com/watch?v=kgCNGvL0g1g
What will I find there?

- David Tennant narrating 2 stories, one of which is about an 11 year-old using an online game to meet people. This could be a video you share with your child to open a discussion on what is safe online behaviour.

Thinkyouknow is an education programme from the National Crime Agency's CEOP Command
Address: www.thinkuknow.co.uk/parents/
What will I find there?
Since 2006, Thinkuknow has been keeping children and young people safe by providing education about sexual abuse and sexual exploitation. It is underpinned by the latest intelligence about child sex offending from CEOP Command. It aims to ensure that everyone has access to this practical information – children, young people, their parents and carers and the professionals who work with them.

For further information, look at Child Exploitation and Online Protection Centre:

http://www.ceop.police.uk/

They also have a site aimed at children, although there is a parent section too.

www.thinkuknow.co.uk

If you would like to discuss any of the issues arising from the information above, please contact the welfare team by emailing safeguarding@steiner-south-devon.org

Compliance:

There is not a legal requirement to restrict such contact, but the school recognises it is in the best interests of the students and staff to have clear and firm boundaries about contact outside of school.