DANESMEAD, FULFORD CROSS, YORK YO10 4PB
TEL: (01904) 654983

York Steiner School E safety policy

Table of Contents

Reporting Incidents

Should an e-safety incident occur please contact:
Maurice Dobie - Designated Safeguarding Lead (DSL)
Fiona Dudley – Deputy Safeguarding Lead & Main School Lead
Karen Foster – Deputy Safeguarding Lead & Early Years Lead

If he is not available and you believe a child to be in danger of serious and imminent harm then please contact the **City of York Council, Children's Front Door on 01904 551900**

Introduction

York Steiner School is dedicated to nurturing each child’s capacity for creative imagination, independent thinking and positive action. The school aims to keep all children safe within its care this extends to providing both parents and children with the necessary information to remain safe in a digital world.

This is a very rapidly developing environment and it is difficult to stay up to date, we therefore encourage a collaborative approach to child safety via education of staff, parents and pupils. If children are taught and encouraged how to remain safe online they are less likely to be the victims of cyber-bullying, grooming, issues around social media or engage in sexting.

York Steiner School recommends no computer access for younger children and limited access, if necessary, for classes 6-8.

We acknowledge that working with parents is a key part of our strategy. The school asks that parents’ guide their children in the appropriate uses of electronic media outside of the school environment. We encourage parents to keep an open dialogue with their children, other class parents and teachers to work out viable approaches

Access to the Internet

At York Steiner School classes 7 & 8 are sometimes allowed internet access in school at the discretion of the teacher to help in studies. We are aware that many students of all ages will have access to the internet at home.

The use of the internet can put young people at risk both within and outside of school. Some of the dangers they may face include:

- 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
- Cybersquatting
- 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.

When children are using computers in school they will be situated in areas of high visibility, this will allow close supervision.

Keeping Children Safe Online

The most effective way to keep children safe is via education. The school implements a detailed e-safety curriculum from Kindergarten upwards to help educate the children. As a secondary means of protection, the list below may be helpful:

- Use filtering technology. Most routers have parental controls, some internet service providers may also offer this service.
- Internet or Web filtering software can prove very effective and give you significant control over which websites are accessible.
- Use the privacy setting within each social media app. Make sure you understand the default settings of each social media platform your child uses and ensure the necessary privacy settings are switched 'on'.
- Encourage a culture of openness and sharing. Talk with your child and let then know you will be checking their history. Don't check every day and become a kind of policeman this will be

counterproductive instead check occasionally showing your child that you trust them however, when you do check, look carefully in case there is something that requires closer scrutiny and more frequent observation.

- Only let your child on computers where you can see them. We would actively discourage parents from allowing their children to disappear into the bedroom with unsupervised internet access.
- Show an interest in the social media apps used and try to understand what each is used for.
- If your child does have social media discuss with them the concept of ‘friends’ and only approving requests people they actually know. Check their friends list occasionally, remember that York Steiner School along with all other schools do not allow staff to be friends with pupils.

Pupil Education

As with all other risks, it is impossible to eliminate the risks completely. It is therefore essential, through good educational provision to build students’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

York Steiner School will ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Staff alongside parents and carers, should consider it to be their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

‘E-safety’ will taught to all children across the whole school from Kindergarten to Class 8 and will be embedded into the curriculum delivered in a variety of ways depending upon the age of the child and/or the needs of the class. The E-safety curriculum covers the following 8 themes:

1. Self-Image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing information
6. Health, Wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

Kindergarten

In Kindergarten we focus on children's strength and emotional resilience to give them balanced social interactions and the opportunity to **connect, be active, give to others, get creative and be mindful.** The Kindergarten environment gives us a lot of opportunities to strengthen children's resilience in this way and we can connect with staff and parents in other parts of the school to support appropriate programmes. Similarly by developing children's creativity, love of the outdoors, handwork, freedom of speech and a sense of awe and wonder we create a counter-balance to technological culture we live in.

Government Policy states that children over the age of 5 need to know:

- What it means to be responsible online
- How to protect your rights online and respect others rights
- How to disengage as well as engage with the digital world

Staff and Parent Education

All staff are encouraged to take the Educare Online Safety course. In addition the DSL will circulate new and relevant information to staff on an ongoing basis during the year.

We are committed to working together with parents on this issue. We invite the Police into school to inform parents about the potential dangers online and we raise parents' awareness of e-safety at parents evenings. Parents build a good relationship with their child's teacher over their 8 year journey and are able to talk openly or raise concerns.

We offer an e-safety training/ awareness evening for parents on an annual basis as well as the topic being discussed during parent's evenings on a regular basis.

Advice for students:

- Don’t publish identifying information.
- Pick a user name that doesn’t include any personal information.
- Set up a separate email account that doesn’t use your real name and use that to register and receive mail from the site. That way if you want to shut down your connection, you can simply stop using that mail account.
- Use a strong password (at least 8 characters; mixture of lower case letters, upper case letters, numbers and symbols).
- Keep passwords safe, and change them regularly.
- Keep your profile closed.
- Only allow friends to view your profile.
- What goes online stays online. Don’t say anything or publish pictures that might cause you embarrassment later. If you wouldn’t say it to your parents, don’t say it online!
- Be on your guard.
- Talk to parents/carers if you feel uncomfortable.
- Save or print evidence.

Advice for parents

- Set ground rules. Discuss. Continue to talk.
- Limit the amount of time online.
- Use ISP filtering.
- Set up a family e-mail account for registering on websites, competitions etc.
- Monitor online activity (recently visited sites, click the History button).
- Software for filtering isn’t fool proof - combine with supervision.
- Check temporary files (open Internet Explorer and select Internet Options, on the General tab under Temporary Internet Files, click the Settings button and the click View Files).
- Contact CEOP or the police if you suspect grooming.

CEOP (Child Exploitation & Online Protection) is dedicated to eradicating the sexual abuse of children, and is affiliated to the Serious Organised Crime Agency (SOCA).

Links with other Policies

This policy should be read in conjunction with all other safeguarding policies as they all work together to safeguard the child, staff and school. These policies collectively support Keeping Children Safe in Education 2018

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies

Any incidents of cyber bullying or other e safety incidents listed in this policy which occur outside of school will still be dealt with in school in line with other polices such as the behaviour policy, child protection policy, the anti-bullying policy. Parent/carers will be informed of such behaviour even if it is out of school.

Safer search engines:

Information on safe search engines can be obtained from the NSPCC: **0808 800 5002**

Further information and advice:

- childnet.com (select 'Know It All' for a wide range of links to other sites)
- NSPCC.org.uk
- getsafeonline.org
- kidscape.org.uk

Useful information can also be found at: https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Control Measures

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider and/ or learning platform.
- Secure email accounts.
- Regularly monitored and updated virus protection.
- A secure password system.
- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use
- Effective audit, monitoring and review procedures.

Social Networking

It is to be recognised that staff are also likely to use social networking sites in their recreational time on their own personal computers.

This form of activity is not to be discouraged however staff must agree and adhere to a 'professional conduct agreement'. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbullying, for example, is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the Designated Safeguarding Officer.

Staff must not have a pupil as a 'friend' or contact on any social networking medium

Review

Approved by the Board of Trustees	December 2018
Policy review date:	December 2019