Oswald Road Primary School

e-Safety Staff Guide

General Introduction

That you so much for you response to the Staff e-Safety Questionnaire- we had a great response. Some staff requested further information so we thought the best way to communicate this would be in a leaflet.

Pro Lifestyle

So-called pro-lifestyle sites are websites (and more commonly information shared on social media) that are normally set up as a peer-support mechanism, but can also promote certain conditions as a good lifestyle choice, such as anorexia and bulimia. These are commonly called pro-ana and pro-mia sites. There are others related to pro-self harm and pro-suicide.

The risk here is such that a young person looking for support on the internet may come across a pro-site instead, and thus be convinced that conditions like anorexia are a good lifestyle choice.

These sites commonly have tips and tricks on how to keep up with such a lifestyle, including masking effects from parents.

Digital Footprint

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. Your digital footprints are made up of the content you create, post and share; as well as the content that others post, and share, with you and about you.

To help you manage and maintain your online reputation we have a simple checklist:

1. **Search yourself online:** do you know what is online about you? Do a simple web search of your name and see what you can find. If you find something you aren't happy with, take the necessary steps to get that content removed. Remember if your Facebook or Twitter pages appear you can change this by adjusting your privacy settings.

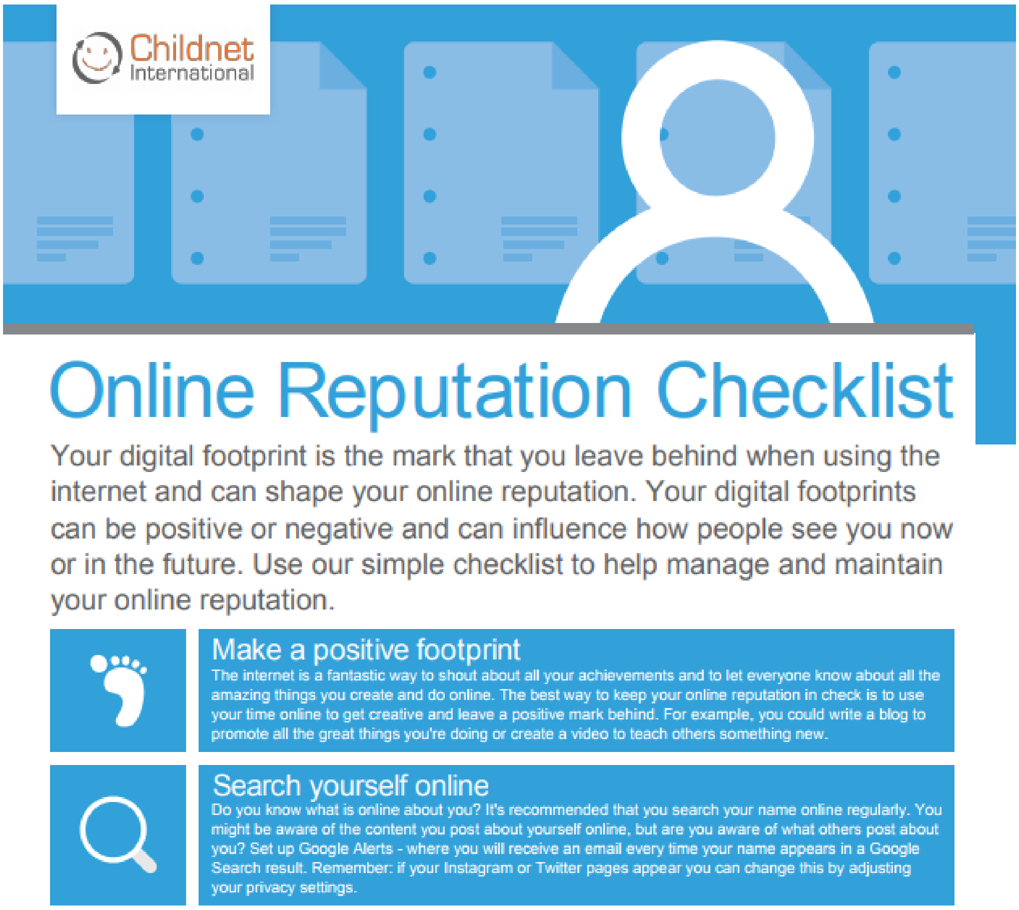
2. **Check privacy settings:** make sure you know what information you are sharing on the websites you use, in particular on social networking sites. Most social networking sites have privacy settings to help you manage the content you share and who you share it with; you can decide if you want your posts to be shared with your online friends and followers only or with the public. Keep in mind that your friend's content and their settings can also affect your digital footprint.

3. **Think before you post:** before you post that funny picture of your friend, or make that joke about someone on Twitter, ask yourself do you want everyone to see it; friends, family, grandparents, future employers? Would you be happy for others to post that type of content about you? You should be proud of everything you post online, remember once it is online it could potentially be there forever!

4. **Deactivate and delete:** when you stop using a social networking profile or website, it's a good idea to deactivate or delete your account. This will mean the content is no longer live and should not be searchable online; it will also remove the risk of these accounts being hacked without you knowing.

5. **Make a positive footprint:** we hear a lot about the negative footprints left behind online. The best way to keep your online reputation in check is to use your time online to get creative and create a positive footprint. For example why not write a blog to promote all the great things you are doing, fundraise for a charity using an online sponsorship page or create a video to teach others something new.

Online Reputation



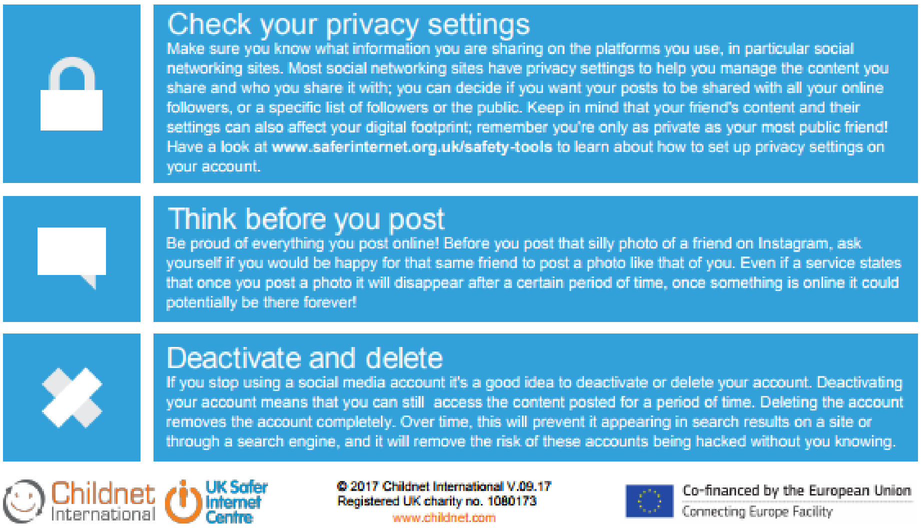
Childnet International

Online Reputation Checklist

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. Your digital footprints can be positive or negative and can influence how people see you now or in the future. Use our simple checklist to help manage and maintain your online reputation.

Make a positive footprint
The internet is a fantastic way to shout about all your achievements and to let everyone know about all the amazing things you create and do online. The best way to keep your online reputation in check is to use your time online to get creative and leave a positive mark behind. For example, you could write a blog to promote all the great things you're doing or create a video to teach others something new.

Search yourself online
Do you know what is online about you? It's recommended that you search your name online regularly. You might be aware of the content you post about yourself online, but are you aware of what others post about you? Set up Google Alerts - where you will receive an email every time your name appears in a Google Search result. Remember: if your Instagram or Twitter pages appear you can change this by adjusting your privacy settings.



Check your privacy settings

Make sure you know what information you are sharing on the platforms you use, in particular social networking sites. Most social networking sites have privacy settings to help you manage the content you share and who you share it with; you can decide if you want your posts to be shared with all your online followers, or a specific list of followers or the public. Keep in mind that your friend's content and their settings can also affect your digital footprint; remember you're only as private as your most public friend! Have a look at **www.saferinternet.org.uk/safety-tools** to learn about how to set up privacy settings on your account.

Think before you post

Be proud of everything you post online! Before you post that silly photo of a friend on Instagram, ask yourself if you would be happy for that same friend to post a photo like that of you. Even if a service states that once you post a photo it will disappear after a certain period of time, once something is online it could potentially be there forever!

Deactivate and delete

If you stop using a social media account it's a good idea to deactivate or delete your account. Deactivating your account means that you can still access the content posted for a period of time. Deleting the account removes the account completely. Over time, this will prevent it appearing in search results on a site or through a search engine, and it will remove the risk of these accounts being hacked without you knowing.

Co-financed by the European Union
Connecting Europe Facility

How to report a concern online

If a child asks to you to report a concern online please see a member of the Safeguarding Team. Dependent on the concern we would sign post to the most appropriate agency.

For in house concerns please report on CPOMS and directly to a member of the Safeguarding Team as a matter of urgency.

Data Protection

As per Sarah Nicholls' email:

There is new legislation coming out next year in relation to data protection which really tightens up the requirements of how we handle data. One of the areas relates to disposal of personal/ confidential data.

Below is a list of questions which can help you decide whether information is classed as 'personal data'. These include:

- Can a living individual be identified from the data, or from the data and other information in your possession, or likely to come into your possession?
- Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?
- Is the data 'obviously about' a particular individual?

- Is the data 'linked to' an individual so that it provides particular information about that individual?
- Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?

Photos of children are classed as personal data therefore need to be disposed of confidentially.

If you have **ANY doubts at all**, please dispose of any paper in the confidential waste containers which are around the school:

- Outside Deb's office
- Outside the studio
- In the main office
- PPA Room
- Nursery

Devices used at home

Devices used at home which contain personal information should be encrypted. If yours is not please do this immediately. If you are unsure how to please see Harvey or a member of the Safeguarding Team.

Professional/Personal Boundaries

As per our e-Safety and Acceptable use policy we would advise:

3.1
In their own interests, adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites, such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

3.2
All adults should review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.

3.3
Adults should never make a 'friend' of a pupil/former pupil at the school where they are working on their social networking page. Adults should also never make a 'friend' of a parent/carer of a pupil/former pupil, unless this person is known to them personally outside of the school setting. Caution should be applied if this is the case and all staff are solely responsible for any content that is published on their social networking pages.

3.4
Staff should never use or access social networking pages of pupils.

3.5
Confidentiality must be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, the school, the governing body, the Local Authority, their colleagues, pupils or members of the public.

3.6
Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Local Authority could result in disciplinary action being taken against them.

3.7
Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on their professionalism.

3.8
Some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee of the school and particularly if you are a teacher or teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school and the profession.

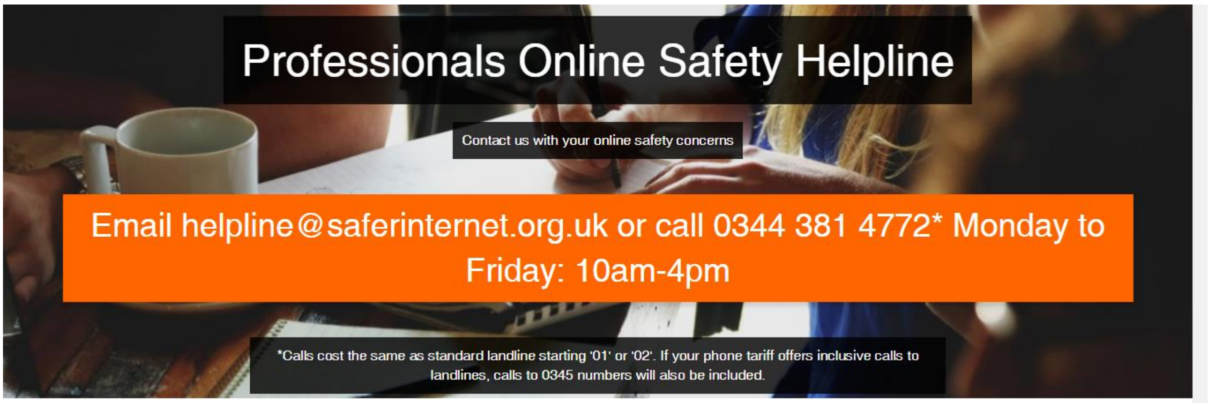
3.9
Adults must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people. All adults are solely responsible for this.

3.10
Any concerns must be raised with the Headteacher or Deputy Headteacher at the earliest opportunity.

New School e-Safety Filter Analysis

Sarah Nicholls has just worked with Harvey to install a new web filter called Barracuda. This allows us to monitor internet usage on all school computers (and laptops when they are logged onto the school server).

Professionals Online Safety Helpline



Professionals Online Safety Helpline

Contact us with your online safety concerns

Email helpline@saferinternet.org.uk or call 0344 381 4772* Monday to Friday: 10am-4pm

*Calls cost the same as standard landline starting '01' or '02'. If your phone tariff offers inclusive calls to landlines, calls to 0345 numbers will also be included.