Twitter...

Twitter is a communications platform that allows users to share small bursts of information called Tweets. Each Tweet is a maximum of 140 characters long. You can also get links, see photos, videos and news stories and participate in conversations using Tweets.

Twitter is a public space

Most of the communication taking place on Twitter is public and viewable by everyone.

While Tweets can be protected so only approved followers can see them, most users share their Tweets with everyone. If your child wants their Tweets to only be available to approved followers, they can protect their Tweets through the Tweet privacy section of their Account Settings.

Source: http://support.twitter.com/articles/470968-safety-tips-for-parents

Facebook...

Facebook is designed for children aged 13 years old and upwards. It allows people to connect with friends and communicate through chat, personal messages and sharing photos, videos, links and other kinds of information. As Facebook is designed for teens, we do not promote its use by children at Highfield Primary School. However, this does not necessarily mean they are not using it. By using a fake date of birth, children under 13 years of age can sign up for a Facebook account. Please take the time to talk to your child about whether or not they are using Facebook and what they are using it for. It is much better that children are open about their use of Facebook, rather than using it secretly.

Who can see my child's timeline?

This depends on the user's account settings. Normally, the people who can see what users under 17 years old post are their Facebook friends, friends of friends, and networks (like the school they attend). Facebook maintain added protections and security settings for teens (age 13-17 years). If children have put in a fake date of birth which gives them an age over 17 years, these security settings may not be applied to their account and their timeline may be visible to more people.

Blogs...

Web-logs, commonly known as blogs, allow people to share their writing with other members of the internet community who can then comment on the work.

The blog could be a diary, research or just pieces of writing they have written for the joy of it. While everyone on the Internet can view this material, if settings are applied correctly, only approved members can contribute a post and all comments must be approved by the blog editor.

The school blogs are managed by class teachers. Children's posts must be approved by the teachers and all comments are moderated by them before being published on the blog.

Social networking safety...

Protect passwords

Explain to your child that passwords should never be shared, not even with their friends. If the home computer is shared, remind them to always log out when they finish their online sessions to develop good online safety habits. It is important to log out of any websites they logged into on a shared computer (to stop other people accessing their information).

Use online safety to connect with your child

Children in particular may feel like parents are disconnected from their perspective and fear conversations about online safety will be awkward or embarrassing. Listen to how your child is using Twitter, Facebook and other online mediums. Take their online relationships seriously.

One of the best ways to begin a conversation is to ask your teens why services like Twitter or Facebook are important to them. You might also ask them to show you how to set up your own Twitter account or Facebook timeline, so you can see what it is all about. Discuss what information it is appropriate to share online - and what is not appropriate. Ask them about privacy settings, and suggest that you go over them together, regularly. Set ground rules, and enforce them.

Keep a healthy life balance

As a parent, you are a role model for your child. Demonstrate the importance of a balance between online and other activities by encouraging family activities online as well as offline.

Social networking safety cont...

Encourage critical thinking

Take the opportunity to learn about the sorts of situations your child is experiencing online, and use these to identify solutions and encourage critical thinking. Ask them questions like:

Who are you sharing this information with?
Can you trust all the people that see the information on your profile?
How could your Tweet/post be interpreted?

Pupils must have a clear understanding of what to do if they have concerns about inappropriate online behaviour (such as unwelcome contact or cyberbullying).

Think before Tweeting/posting

As parents, you may have seen children say or write things that were not meant to be hurtful but that others found offensive or upsetting. Help your child evaluate whether or not something is okay to post by reminding them that if they would not say it to the person's face or out loud, they should not say it online either.

The nature of the Internet makes it difficult to erase content completely. Consider having a conversation about how what gets posted online can hurt feelings, affect offline relationships and even jeopardise future opportunities.

It is about respect

It is also important to talk about the Golden Rule: treating others the way you want to be treated. This also applies to using new technologies. Make sure your children know where to go for support if someone ever harasses them. Help them understand how to make responsible and safe choices about what they post - because anything they put online can be misinterpreted or taken out of context.

Dealing with problems...

Spam

Some people take advantage of the fact they can send messages to lots of people in an online community. Users of social networks may find they receive confusing messages from strangers, perhaps trying to sell products or open communication. This is known as spam. If users receive spam, they should block that user so they can no longer communicate with them. If the messages continue, they should be reported to the specific site.

Spam can also be used to launch 'phishing' attacks where users are sent emails tricking them into 'updating' their personal details online via a fake website (imitating a bank or similar) or through a misleading pop up advertisement - such as a banner informing that you have won a prize or money.

Spam can also be used as a means of distributing malicious software ('malware') which has been designed to secretly access a computer network or system, without the owner's consent. Once there, malware usually causes some unexpected and undesirable result, ranging from being intrusive or annoying (in the case of 'adware'), to compromising your personal information (in the form of keystroke-logging spyware used for identity theft), or outright destructive (in the form of viruses which might destroy system files or impact upon the operation of your system).

There are a number of strategies that parents can employ, in combination, to guard against spam, malware and viruses. These include technological protection in the form of firewalls and anti-virus software on the home network, and awareness and education for all family members.

When it has gone too far...

Sometimes, people can use social networks to 'bully' other users. If unwanted online behaviour is persistent, it may be rooted in 'real world' relationships. If your child is experiencing repetitive cyber-bullying or interpersonal conflicts that are also taking place online, consider taking the following actions:

· ## Coordinate with the school
Many issues can be resolved by working with staff at Highfield or through another authority the school has contact with, such as CEOP. If your child is experiencing repetitive cyber-bullying, please contact the school for support in taking action. If the perpetrators of the bullying are found to be pupils of the school, we will deal with the situation in the same way we would physical bullying.

· ## Report a violation
Get to know the Twitter / Facebook rules and policies. After reviewing their policies, if you believe an account is violating their rules, you or your child can file a report.

· ## Contact local law enforcement
Twitter and Facebook will investigate every report received, but if something has gone beyond the point of a personal conflict and has turned into credible threats, whether it be online or offline, you should contact your local authorities as they are in the best position to assess the threat and intervene or assist as necessary.

Support from external agencies...

Telling a parent or teacher should normally be the first response to unwanted online behaviour, but children should also know that they can talk directly and confidentially to *Childline* (tel.: 0800 1111 or www.childline.org.uk) about such matters or report potential online abuse to the Child Exploitation and Online Protection Centre (CEOP).

Further advice and guidance on social networking and e-safety for children and parents/carers is available from the following sites:

CEOP's *Thinkuknow*	www.thinkuknow.co.uk
Childnet	www.childnet.com/resources/young-people-and-social-networking-sites
KnowItAll	www.childnet.com/resources/kia/
Kidsmart	www.kidsmart.org.uk/
UK Safer Internet Centre	www.saferinternet.org.uk/
Chatdanger	www.chatdanger.com/
Digizen	www.digizen.org/

Tips for parents/carers...

Some suggestions of how to support your child's internet use:
1. It can be tough to keep up with technology. Do not be afraid to ask your child to explain it to you.
2. If you are not already on Facebook or Twitter, consider joining. That way you will understand what it is all about!
3. Teach your child the online safety basics so they can keep their online accounts private and safe.
4. Talk about technology safety just like you talk about safety while out alone or playing sports.

Start a conversation with your child

Some suggested ways of starting a conversation with your child about their social networking:

1. Do you feel like you can tell me if you ever have a problem at school or online?
2. Help me understand why Facebook/Twitter is important to you.
3. Can you help me set up a Facebook timeline/Twitter account?
4. Who are your friends on Facebook?
5. I want to be your friend on Facebook. Would that be OK with you? What would make it OK?

Our Anti-Bullying Ambassadors made a video which you can find on our website, please take time to watch this with your child

Glossary...

@
The @ sign is used to call out usernames in Tweets, like this: *Hello @Twitter!* When a username is preceded by the @ sign, it becomes a link to a Twitter profile.

Avatar or Profile Picture
The personal image uploaded to your Twitter profile in the *Settings* tab of your account.

Blog
A discussion or informational site published on the World Wide Web and consisting of discrete entries (or 'posts') typically displayed in reverse chronological order.

Chat
Chat is a feature that lets you send instant messages to online friends.

Follow
To follow someone on Twitter is to subscribe to their Tweets or updates on the site.

Follower
A follower is another Twitter user who has followed you.

Following
Your following number reflects the quantity of other Twitter users you have chosen to follow on the site.

Friends
Friends are people you connect and share with on Facebook.

Hashtag
The # symbol is used to mark keywords or topics in a Tweet. It was created organically by Twitter users.

Messages
Your messages and messages inbox house your on-going conversations with people on Facebook.

Poke
When you poke someone, they will receive a notification that you have poked them. People poke their friends on Facebook for a variety of reasons. For instance, you can poke your friend just to say 'hello'.

Timeline
Your timeline is your collection of the photos, stories and experiences that tell your story.

Trends
A subject algorithmically determined to be one of the most popular on Twitter at the moment.

Tweet
Tweet, tweeting, tweeted. The act of posting a message, often called a 'Tweet', on Twitter. A message posted via Twitter containing 140 characters or fewer.

Wall
Your Wall is the space on your profile where you and friends can post and share.