Bolton Council

USE OF SOCIAL NETWORKING SITES – GUIDANCE FOR STAFF / VOLUNTEERS

Schools

April 2011

CONTENTS

1 INTRODUCTION

Technology is integral to the lives of children and young people in today's society, both within school and outside of school. The internet and other information and communication technologies are powerful tools – they open up new opportunities for everyone, promoting discussion, creativity and effective learning. They also bring opportunities for staff to be more creative and productive in their work.

1.1 Statement of Intent

"……School is committed to safeguarding and promoting the welfare of children, young persons and vulnerable adults and we expect all staff and volunteers to share this commitment."

1.2 Social Networking: Principles

Online social networking and interactive services can provide extensive benefits to their users. However while staff and volunteers will want to make the most of these services, this document aims to ensure they understand the importance of protecting themselves, their online identities and their reputations. One set of information can and will influence the other to create a single digital footprint that can equally be detrimental or supportive of the School / Council or the individual.

"*Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny." DCSF Nov 07*

"All adults working with children and young people have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of the public in general and all those with whom they work. There may be times, for example, when an adult's behaviour or actions in their personal life come under scrutiny from local communities, the media or public authorities. This could be because their behaviour is considered to compromise their position in their workplace or indicate an unsuitability to work with children or young people." Guidance for Safer Working Practice for Adults Who Work with Children and Young People.

1.3 Standards

This document requires everyone who works, paid or unpaid (staff, Governors, volunteers etc), with children and young people to uphold the standards included within this document, including:

- To behave online in a professional and appropriate manner
- To be a 'responsible user' and stay safe whilst using technology
- To ensure work ICT systems are protected from accidental or deliberate misuse
- That staff and volunteers always have the duty of care to pupils as their main priority
- That the school / Council are not exposed to legal and governance risks;

The law states that if an action is illegal offline it is also illegal online. This applies both to issues such as distributing illegal material and also to harmful behaviour if it amounts to a course of harassment or grooming.

All staff / volunteers should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

It is vital that staff / Governors / volunteers are aware of the importance of keeping private and professional information separate. Irresponsible use of new technologies can affect your reputation, your self-esteem, your health and, in some cases, your career progression.

The standards set in this document apply to all electronic devices including PDA's, laptops, mobile phones, USB devices etc.

The document "Guidance for Safer Working Practice for Adults Who Work with Children and Young People" states that *"Adults should not behave in a manner which would lead any reasonable person to question their suitability to work with children or act as a role model."*

A list of useful contacts is detailed in Appendix 1.

2 SOCIAL NETWORKING – WHAT IS IT?

Social networking sites allow users to create their own content and share it with a vast network of individuals, and potentially the world. Some examples of popular sites include:

- Facebook
- Bebo
- Friends Reunited
- LinkedIn
- MySpace

New sites are being developed and launched on a daily basis, however the main site in use today is Facebook.

More than a third of adult internet users in the UK have a profile on a social networking site.

2.1 Facebook

Facebook has gained over 500 million users since it was launched in 2004, about one in 14 people of the world's population. Many organisations now use Facebook to communicate with potential customers / staff, including the British Army, KPMG and Starbucks.

Facebook allows users to keep in touch with friends and colleagues by posting status updates, writing on their "wall", emailing or even giving them a "poke" to say hello. Users can also "tag" friends in photo's, share music and video clips, and join or set up similar interest groups or fan pages. Facebook also has an instant messaging service where you can chat with friends.

2.2 Other Social Networking Sites

LinkedIn has over 80 million users across 200 countries. Users are able to connect with colleagues, recruiters and mutual contacts. You can build up a network of direct connections and extend your network to include connections of existing contacts, follow different employers and get notified when they have vacancies, and post questions and blogs for the community to answer.

Twitter, which launched in 2006, has more than 175 million users. Twitter enables you to send and read "tweets" : text-based posts of up to 140 characters. You can follow other subscribers' "tweets", such as celebrities. Many large employers, including HSBC, IBM and Pepsi Co are tweeting new jobs to potential recruits.

Bebo is similar to Facebook and currently has 117 million registered users. It was launched in 2005 and was owned by AOL. Bebo is an acronym for *Blog Early Blog Often*. Users receive a personal profile page where they can post blogs, photographs, music, videos and questionnaires to which other users may answer. Additionally, users may add others as friends and send them messages, and update their personal profiles to notify friends about themselves.

Screen shots of some of the most popular sites are show in Appendix 2.

3 SOCIAL NETWORKING AND CHILDREN & YOUNG PEOPLE

Most children and young people use the Internet positively but some behave in ways that place them at risk. Some of these actions to them seem harmless, but could expose them to potential harm. A young person can be a victim of online abuse through exposure to harmful content and cyber bullying. These situations can quickly escalate to a point where the young person may lose control. Potential risks to children and young people using social networking and other user interactive services can include, but are not limited to:

- Bullying by peers and people they consider 'friends'
- Exposure to inappropriate and/or harmful content
- Involvement in illegal or inappropriate content
- Posting personal information that can identify and locate a child offline
- Theft of personal information
- Sexual grooming, luring, exploitation and abuse through contact with strangers

This emphasises the need for children and young people to be educated about the appropriate and responsible use of the Internet. It is important to point out to children and young people that content posted online can impact their reputation, both positively and negatively, now or in the future.

Social networking sites can be used to:-

- Meet known friends and make new friends
- Experiment with their identity and opinions
- Have a 'place' or 'space' where parents or carers may not be present
- Upload and share images of themselves, their family and friends

- Upload and share videos
- Create blogs, journals or diaries about their lives
- Play online games
- Receive comments or messages from friends or guests
- Create or join wider communities or interest groups, i.e. football or music.

These sites are very popular with children and young people. Key attractions are the ability to create original and personal content, to express themselves and connect and communicate easily with others. They use social networking and interactive sites as an extension of their offline lives, and many do not distinguish between the online and offline environments.

Over half of all 8 to 17 year olds with access to the Internet have a profile on a social networking site. Many of these sites set a minimum age limit of 13, however young people below this age are able to register with these sites by inputting a false date of birth.

3.1 Contact with Children & Young People

It is not appropriate for representatives of the School / Council to have clients / those for which they have a duty of care who are under the age of 18 (i.e. pupils) as 'friends' on such sites. Staff / Governors / volunteers who have records on social networking sites should ensure the highest level of security is in place and that they do not either accept a 'friend request' or make a 'friend request' to any person under the age of 18 years to whom they have acted 'in a position of trust', or someone who is over the age of 18 to whom they are still acting 'in a position of trust', i.e. sixth form pupils.

Those who work with children and young people are at an increased risk of allegations being made against them. It is therefore vital that staff and volunteers take appropriate steps to protect themselves from allegations, and to ensure appropriate behaviour both online and offline.

There is an uneven power base between staff / Governors / volunteers and young people, in which adults have authority over students / clients (current and former) which continues to shape those relationships.

The relationship with pupils / clients should at all times remain professional, and staff / Governors / volunteers must not correspond with pupils / clients through such sites or add them as 'friends'. All staff / Governors / volunteers are responsible for their own actions and behaviour and should avoid any contact which would lead any reasonable person to question their motivation and intent.

3.2 Abuse of Children & Young People

As well as the risk of bullying, children who use social networking sites are also at risk of accessing information and chat rooms which promote and/or incite risk-taking or dangerous behaviours, self-harm, suicide and eating disorders. Young people seek opportunities to express themselves, and therefore may choose to upload content relating to these behaviours. This can be a positive experience for young people dealing with life's challenges, however there can be negative or worrying aspects of this exploration and engagement which can manifest themselves in the apparent promotion or encouragement of self-harm, e.g. filming and publishing these activities.

There is also concern that social networking may increase the potential for sexual exploitation of children and young people by adults, or by other young people. This exploitation can include:

- Exposure to harmful content, including adult pornography and illegal child sexual abuse images
- Engaging in sexually explicit communications and conversations that may reduce children and young people's inhibitions
- Manipulation and exploitation, which can include being encouraged or paid to pose in sexually provocative ways and pose naked and/or perform sexual acts via webcams, and
- Grooming and luring of children to meet offline to sexually exploit them

3.3 Bullying and Harassment

As well as young people bullying their peers, some adults (particularly teachers) have also found themselves targets of online abuse and harassment. This has caused some concern within schools, not only about the individuals depicted in postings, but also the reputation of the school. In some instances, these situations have resulted in investigations being initiated by the Police and Education Authorities.

Examples of bullying include personal intimidation, impersonation, exclusion, posting images of bullying incidents, stealing a password to take over a user's page, making false reports to the service provider.

3.4 'Grooming'

Grooming is a process by which someone makes contact with a child with the motive of preparing them for abuse, either online or offline. Abusers can use public online interactive spaces to find and meet children and young people, and they can be exploited online without actual physical contact taking place in the real world, e.g. by sending and exchanging sexual images, and/or by persuading children and young people to send explicit images of themselves.

There have been a number of cases where adults have used social networking services as a means of contacting and grooming children and young people for sexual exploitation. Abusers use a range of techniques to make contact and establish relationships with children and young people, including:

- Gathering personal details such as age, name, address, mobile number, name of school and photographs
- Offering opportunities for modelling, particularly to young girls
- Offering material gifts including electronic games, music and phone credit
- Offering virtual gifts such as rewards, passwords and gaming cheats
- Gaining a child's confidence by offering positive attention and encouraging the child to share or talk about any difficulties or problems at home, and providing a sympathetic and supportive response
- Bullying and intimidating behaviour, such as threatening to expose the child by contacting their parents to inform them of their child's communications or postings on a social networking site and / or saying they know where the child lives or goes to school
- Asking sexually themed questions, such as 'do you have a boyfriend'? or 'are you a virgin?'

- Asking children and young people to meet offline
- Sending sexually themed images to a child, depicting adult content or the abuse of another child
- Masquerading as a minor or assuming a false identity to deceive a child

Having made contact with a child or young person, abusers may also use that young person as a means to contact and get to know their friends using the links to their 'friends' in user profiles.

Many young people find it extremely difficult to seek help or disclose their abuse because of their sense of personal responsibility, feelings of guilt or shame, and fear that they may not be believed or may be 'blamed' and lose access to the Internet.

4 SECURITY OF YOUR SOCIAL NETWORK INFORMATION

4.1 Security Settings

It is vital that when you register to become a user of a social networking site, you ensure that you access the 'settings' page and set these to their highest possible level. This will ensure that only those people who you authorise to see your information will be able to see it, however remember that friends may respond to your comments, or post comments on your photographs which their friends are then able to see, and so on.

4.2 Friend Requests – Sending & Receiving

Under no circumstances must staff / Governors / volunteers accept friend requests from children / young people, nor should they make such requests. Should a young person attempt to contact you in this way, you should make this known to your manager immediately.

4.3 Remote Access to Social Networking Sites

Many staff / Governors / volunteers and young people now have the facility to access their social networking information 'on the move' and can keep it updated at all times via mobile phones, I-Pads etc. It is vital that these items are password protected to the highest level to avoid unauthorised access / use. Guidance should also be issued to staff / pupils on accessing such sites during working / teaching hours.

4.4 CEOP

The Child Exploitation and Online Protection Centre (CEOP) have launched a national campaign 'Think U Know'. This campaign provides young people with advice and guidance on how to have fun, stay in control of their personal information and report any problems they may encounter in the online environment.

CEOP and Facebook have developed a new free application or 'app' that will make young people safer within Facebook. 'ClickCEOP' is a new 'app' which links the young user and parent directly from their Facebook home page to help, advice and reporting facilities of the Child Exploitation and Online Protection (CEOP) Centre. Further information on how to do this is contained within Appendix 3.

5 DO'S & DON'TS

Online profiles are lots of fun and can be a great place to share your interests, communicate with friends and learn new skills. However, as in the real world, it is important that you take care of yourself, your friends and the wider community.

Information you post will reflect the kind of person you are, and will influence what others think of you. What is your content saying about you?

A survey in 2009 found that more than a quarter of British office workers aged 18-29 were spending three or more hours per week when at work on social networking sites, with a massive 42% of young office workers discussing work-related issues on those sites.

- **Do**
  - Think about who you want to see your personal information
  - Read the privacy settings information carefully
  - Set your profile to 'private' / the highest security setting
  - Review your 'friends' list regularly to ensure you still want them to know your personal details
  - Think very carefully about what you share with friends, even if your information is 'private' as this may appear on your 'friends' page
  - Protect your password and never share it with anyone else
  - Protect your mobile phone with a PIN in case it gets lost or stolen, and so that your social networking account is further protected
  - Only communicate with pupils via official school / council systems
  - Be careful about the kind of information (including images) you share about yourself and how you manage your online reputation. Other people can pass on or change your information and you might not be able to stop them or delete it afterwards.
  - Guard your online reputation
  - Comply with the codes of conduct of both your employer and of any professional body to which you belong
  - Use a strong password – numbers as well as letters, and never let anyone else have it

- **Don't**
  - Share information that shows you or your friends in a compromising situation
  - Post images of yourself posing in a sexual or provocative way
  - Post images which include other people without seeking their permission first
  - Post content that may be seen as racist, homophobic, bullying or threatening
  - Set up a fake page to pose as someone else – this can have very serious consequences
  - Bring the school / Council into disrepute by posting derogatory comments about your work / employer
  - Put yourself in a position of vulnerability whereby your motivation and intentions can be questioned
  - Access social networking sites from Council / School computers
  - Access social networking sites from personal mobile telephones / devices during working hours

- Use personal equipment, i.e. mobile phones or cameras to take photographs of children and young people
- Use a personal mobile phone to contact young people, either by phone or text
- Give any personal details, including your mobile number, to a young person

- **Remember**
  - You are not anonymous online. Every computer and device connected to the Internet has a unique address (given by your Internet service provider). This is linked to your computer in the real world – to your real-world address
  - What may seem funny to you can actually be very hurtful and offensive to others
  - Think carefully before you post so you don't embarrass yourself or your friends
  - Be a good friend and, if your friends are behaving inappropriately, remind them that they are not anonymous and can be traced
  - The Internet is a very public place, and inappropriate postings may result in public humiliation, hurt or distress beyond what you ever intended
  - The school / Council will monitor your Internet and email usage to ensure it is being used for the purpose for which it was intended

6 SOCIAL NETWORKING: ROLES AND RESPONSIBILITIES

6.1 Chair of Governors

The Chair of Governors is responsible for:

- Ensuring the school has an effective and operational social networking policy
- Ensuring mechanisms are in place to appropriately protect and monitor school ICT systems
- Reviewing the school's ICT security in light of information / concerns that may arise
- Ensuring that any concerns or allegations are dealt with appropriately in line with recognised procedures

6.2 Head Teachers / Managers

Head Teachers / Managers are responsible for:

- Ensuring that all staff / volunteers within the workplace have signed a copy of this document, and that a copy is always on display in the staff room
- Ensure that child protection training includes a reminder around social networking responsibilities
- Ensuring any concerns / complaints made by staff or young people are dealt with in line with recognised procedures
- Ensuring allegations are not discussed further until advice has been sought
- Ensuring children and young people understand the advantages and disadvantages of social networking, and how to keep themselves 'safe'

6.3 Individuals

All staff, Governors and volunteers are responsible for reading and signing a copy of this document as confirmation of receipt and acceptance.

Staff, Governors and volunteers are responsible for protecting the identity / personal information of the children and young people for whom they have a responsibility, and must ensure that this information is retained in line with the principles of the Data Protection Act. No information should be kept at home / in vehicles – all information should be locked in secure storage devices at school.

Should you disclose confidential information, breach data protection obligations, fail to obtain consent before making a comment public, perpetuate a libel or harm the organisations reputation or business interests, this will be treated as misconduct under the appropriate disciplinary procedure. In serious cases it could be treated as gross misconduct and could lead to dismissal.

APPENDIX 1

Contacts / Useful Organisations

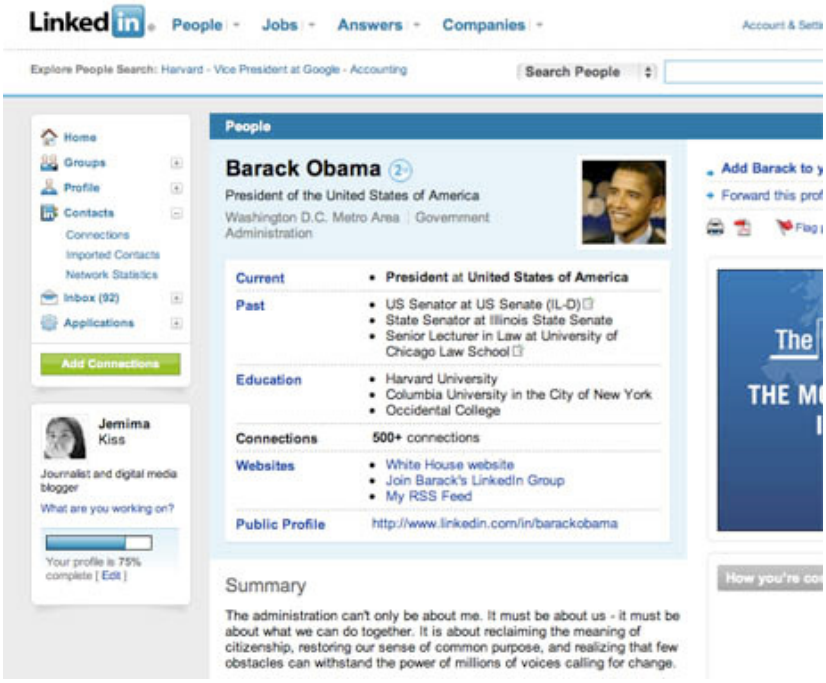
- www.ceop.gov.uk
- www.thinkuknow.co.uk
- www.internetsafetyzone.co.uk
- www.nch.org.uk
- www.nspcc.org.uk/helpandadvice
- www.childline.org.uk
- www.bbc.co.uk/chatguide
- www.childnet-int.org/blogsafety/teachers.html
- www.nextgenerationlearning.org.uk/safeguarding
- www.teachtoday.eu/
- www.boltonsafeguardingchildren.org.uk
- www.getnetwise.org
    - http://kids.getnetwise.org/safetyguide/technology/facebook/facebook-private-audio (facebook privacy settings guidance)
- www.facebook.com/clickceop
- http://www.connectsafely.org/
    - www.connectsafely.org/fbparents
    - http://www.connectsafely.org/Safety-Advice-Articles/facebook-privacy-chart-for-teens.html
- http://www.education.gov.uk/schools/pupilsupport/behaviour/bullying/cyber/a0010037/cyberbullying-checklist

This page can be sent electronically on request

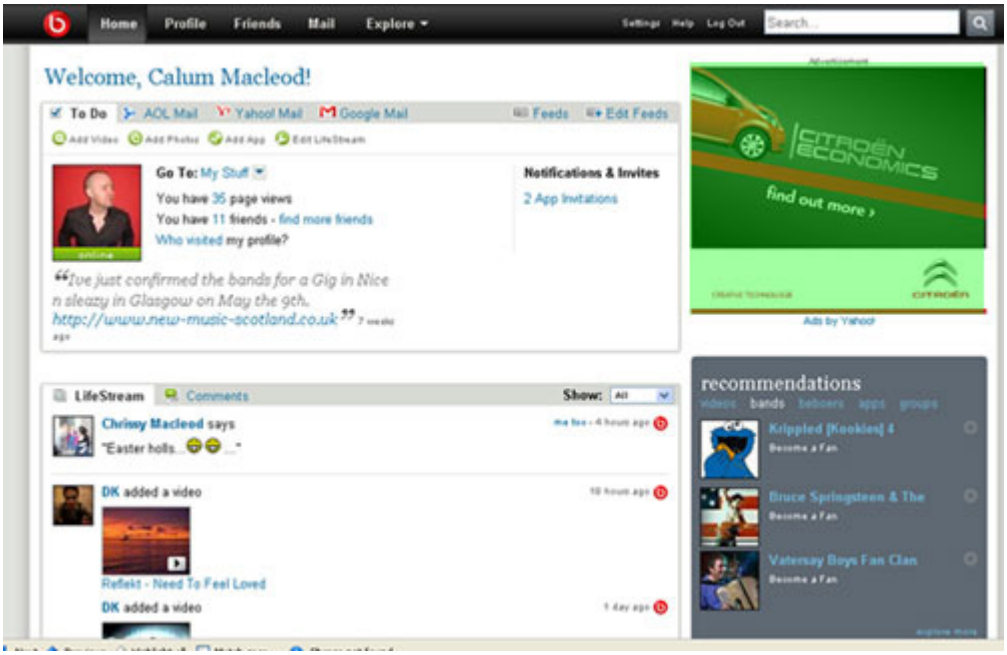
APPENDIX 2


flickr
facebook
twitter
LinkedIn


facebook
Remember Me
Forgot your password?
Email
Password
Facebook helps you connect and share with the people in your life.
Sign Up
It's free and anyone can join
Full Name:
Your Email:
New Password:
I am:
Select Sex:
Birthday:
Month:
Day:
Year:
Why do I need to provide this?
Sign Up
To create a page for a celebrity, band or business, click here.


LinkedIn
People
Jobs
Answers
Companies
Explore People Search: Harvard - Vice President at Google - Accounting
Search People
Home
Groups
Profile
Contacts
Connections
Imported Contacts
Network Statistics
Inbox (92)
Applications
Add Connections
Jemima Kiss
Journalist and digital media blogger
What are you working on?
Your profile is 75% complete [Edit]
People
Barack Obama
President of the United States of America
Washington D.C. Metro Area | Government Administration
Add Barack to
Forward this
Current
President at United States of America
Past
US Senator at US Senate (IL-D)
State Senator at Illinois State Senate
Senior Lecturer in Law at University of Chicago Law School
Education
Harvard University
Columbia University in the City of New York
Occidental College
Connections
500+ connections
Websites
White House website
Join Barack's LinkedIn Group
My RSS Feed
Public Profile
http://www.linkedin.com/in/barackobama
Summary
The administration can't only be about me. It must be about us - it must be about what we can do together. It is about reclaiming the meaning of citizenship, restoring our sense of common purpose, and realizing that few obstacles can withstand the power of millions of voices calling for change.


twitter
1 new friend request
Add or invite friends
Phone Alerts
ON OFF
A WHOLE WORLD IN YOUR HANDS
To update: text to +14152838611
All public updates (over the last 24 hours)
Liz Ugh! Loud coworker male walking the hall talking and joking to someone else while I'm on a business call! I can't freaking hear! Makes me so mad! &+!$#!
2 minutes ago from mobile
Jessica Pete I drop you a comment on your blog, that was a really cool site :)
10 minutes ago from web
Jessica ohhh lunch time :) 10 minutes ago from web
james from the last meeting..."nothing is more frustrating than silent failure"
13 minutes ago from web
Pete Where's your blog Richard? I gave Twitter a review in my blog today also (xanga.com/pedrothepoet) 18 minutes ago from web
Richard Giving twitter a write-up on my blog. Still feeling ashamed for the typo in my last update. 23 minutes ago from web


Home
Profile
Friends
Mail
Explore
Welcome, Calum Macleod!
To Do
AOL Mail
Yahoo! Mail
Google Mail
Feeds
Edit Feeds
Go To: My Stuff
You have 35 page views
You have 11 friends - find more friends
Who visited my profile?
Notifications & Invites
2 App Invitations
"I've just confirmed the bands for a Gig in Nice n sleazy in Glasgow on May the 9th. http://www.new-music-scotland.co.uk"
CITROËN ECONOMICS
find out more ›
Ads by Yahoo!
LifeStream
Comments
Show:
Chrissy Macleod says
"Easter holls..."
DK added a video
Refekt - Need To Feel Loved
DK added a video
recommendations
bands
Krippled [Kookies] 4
Bruce Springsteen & The
Vaterray Boys Fan Clan

APPENDIX 3

FACEBOOK & THE CHILD EXPLOITATION AND ONLINE PROTECTION CENTRE

CEOP and Facebook have developed a new free application or 'app' that will make young people safer within Facebook. 'ClickCEOP' is a new 'app' which links the young user and parent directly from their Facebook home page to help, advice and reporting facilities of the Child Exploitation and Online Protection (CEOP) Centre

The 'ClickCEOP' app is a three stage application that asks young people to: -

- Add the app – and the ClickCEOP tab will appear at the top of your profile page
- Share the badge – and you can share the app with your friends via their newsfeeds
- Bookmark the app – and an icon will appear on your profile page making it easy for you to access the help and advice from the ClickCEOP app.

By adding the app, young people and parents can get support from CEOP on a range of issues – viruses, hacking, dealing with bullying online and they can report someone who is acting inappropriately towards them online.

The 'app' is the outcome of collaboration between CEOP and Facebook who have combined Facebook's expertise in connecting and communicating online with CEOP's expertise in helping young people stay safe.

Once added to their profiles, young users will receive regular messages from CEOP and its partner organisations who operate 'behind the button' to make children safer. CEOP's new Facebook page (www.facebook.com/ClickCEOP) will also contain polls, news alerts and status updates. The page will look at topics that teenagers care about, such as celebrities, music and exams and will link these subjects to questions about online safety. The move is also being supported by an advertising campaign on Facebook that will encourage take up. This will include an automatic advert appearing on every profile of users aged between 13-18 years inviting them to add the app.

If you work with children or young people, please share the information with them and get them to search 'ClickCEOP' in Facebook and give them to chance to be one click away from help – *if* they should ever need it www.facebook.com/clickceop

APPENDIX 4

DfE Guidance on Cyberbullying

Dealing with cyberbullying is best done within a robust framework of policy and practice that includes and supports the whole-school community.

Every school should ensure

- school governors, headteachers, and senior management team members are familiar with the Government's *Safe To Learn cyberbullying guidance*
- the whole-school community understands what is meant by 'cyberbullying', its potential impact, how it differs from other forms of bullying and why it is unacceptable
- all staff are provided with information and professional development opportunities regarding understanding, preventing and responding to cyberbullying – it is particularly important that they understand child protection and other legal issues that may relate to cyberbullying incidents
- current school policy, guidance and information relevant to cyberbullying is reviewed to ensure it meets the needs of pupils and staff. These are likely to include:
    - behavioural agreements
    - acceptable use policies including the use of mobile phones and cameras within school
    - employee terms and conditions
    - pupil and staff support and pastoral care.
- the whole-school community understands reporting routes and responsibilities. A member of the senior management team should be appointed to lead on and oversee anti-cyberbullying activity and incidents. Staff may find it difficult to report instances of cyberbullying to their manager, and they should feel free to seek advice from agencies outside school – their union or professional association, for example, or the Teacher Support Network
- the positive use of technology, which models safe and effective practice, is key to preventing the misuse of technology
- learning strategies and targets, as well as staff development programmes, support the innovative and engaging use of technologies
- the impact of prevention and response policies and practice is monitored annually
- staff, pupils and parents feel confident that their school effectively supports those who are cyberbullied.

School employees should expect:

- all incidents that they report are recorded
- the school will respond to an incident in a timely and appropriate manner where possible, or support the member of staff concerned to do so
- appropriate personal support, or information enabling them to access appropriate personal support will be provided
- information on the safe use of technology will be provided to them
- the school will approach third party agencies on their behalf in order to request that inappropriate material is removed, where possible
- the school will support the staff member in cases where it is necessary for the person being bullied to contact the service provider directly, for example where identity theft or impersonation has taken place, where an individual has a complaint about their appearance in a video, or where the incident involves contacting the staff member's mobile phone service provider
- where appropriate, the school will contact the police or their local authority designated officer (LADO).

Where the bully is a member of the school community, employees should expect:

- the school will work with and take steps to change the attitude and behaviour of the bully
- the school will take care to make an informed evaluation of the severity of the incident, taking into account ways in which cyberbullying differs from other forms of bullying
- the school will deliver appropriate and consistent sanctions.

School employees should take steps to protect themselves and their personal information by:

- keeping passwords secret and protecting access to their accounts
- not befriending pupils on personal social networking services
- keeping personal phone numbers private and not using their own mobile phones to contact pupils or parents
- keeping a record of their phone's unique International Mobile Equipment Identity (IMEI) number, and keeping phones secure while on school premises
- not posting information about themselves publicly that they wouldn't want employers, colleagues, pupils or parents to see
- ensuring that rules regarding the use of technologies are consistently enforced
- not personally retaliating to any incident
- reporting any incident to the appropriate member of staff in a timely manner
- keeping any evidence of an incident.