ONLINE SAFETY: PROTECTING SCHOOL STAFF AND PUPILS

NEU Guidance for Members, Reps and Local Officers

PROTECTING SCHOOL STAFF

Online safety is a key issue for all schools as it can pervade all aspects of school life. Staff in schools, as well as pupils, may become targets of cyberbullying. Cyberbullying is a whole school community issue. It takes place when an individual or group of people use technology such as social media to bully, threaten or embarrass their victim. It is important that schools make it clear that bullying including cyberbullying of staff is unacceptable.

Though online safety is not just confined to cyberbullying of course, cyberbullying is best dealt with within a robust framework of policy and practice, which includes and supports the whole-school community. In their guidance on cyberbullying, the DfE state that 'all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff and supporting them if it happens'.

The NEU believes, therefore, that every school should have a policy on online safety, which should cross-refer to other policies dealing with bullying/harassment, pupil behaviour and child protection. Supplementing this guidance, at Appendix 1, is a model policy which employers should be encouraged to adopt, where an equivalent policy is not already in place.

When responding to incidents, the NEU believes that the practice of searching the contents of pupils' phones is unlikely to be used other than rarely due to its impracticability and the damage it could do to teacher/pupil relationships. The NEU believes that schools will be best served by including clear statements within their behaviour policy about the situations in which this may be done, after consulting fully within the school community. Any teachers or school staff who are to be asked to undertake such searches, which the NEU believes will only be in exceptional circumstances, should be given full guidance and any necessary training. It is of utmost importance that individual school staff operate fully within the school's procedures. More information is available in the NEU health and safety briefing Searching Pupils for Prohibited Items, available on the NEU website, https://neu.org.uk/.

School staff need to be aware of their online reputation and have to recognise that their online activity can be seen by others particularly when using social media. The UK Safer Internet Centre provides help for staff on how to stay safe online, as well as how to support young people in staying safe. It is funded by the European Union and provides a helpline for professionals who work with children and young people in the UK, specifically tackling online safety. The helpline is available at helpline@saferinternet.org.uk and 0844 381 4772. In relation to young people, help is available on safe use of social networking sites, cyber-bullying, sexting and child protection issues. School staff can also obtain advice about protecting their own on-line reputation. The helpline operates between 10am and 4pm, Monday to Friday.

There are also workload issues associated with technology in schools. Time to read and respond to e-mails should be incorporated into a teacher's directed time budget, as part of their other professional duties. Teachers and school staff should not be expected to deal with their e-mail correspondence in the evenings or at weekends. Senior management in particular need to recognise that any electronic communications they may send to teachers and staff in the evening or at weekends will not necessarily be responded to until the next available working day. There should also be no expectation on the part of management, pupils or parents that instant replies will be sent.

‘Sexting’ incidents in schools

‘Sexting’ is a broad term which can refer to a variety of behaviours, but for the purposes of this guidance for schools, the term is used to refer to ‘images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature, or are indecent’.

The high numbers of young people with smart phones and tablets creates opportunities for them to produce and share such images. Indeed, teenagers may think of sexting as ‘mundane’ and a common behaviour. Sometimes this behaviour can be part of a romantic relationship between young people; however, sexting can also be coercive and/or exploitative, and images can be used to bully and blackmail children.

In regards to the law, the production and sharing of such images is illegal, although the response to a sexting incident is likely to vary depending on a variety of factors, including the age of the children involved, whether the image has been distributed more widely, if any coercion was involved and if the child is considered vulnerable or at risk.

In a recent case, a young boy of 14 was added to a police database after sending an image of himself to a classmate. This raised concerns that young people may be criminalised for behaviour they were not aware was illegal. In response to these concerns, the Association of Chief Police Officers has stated that they do not want to criminalise young people, and will only undertake prosecutions in exceptional circumstances. However, as the repercussions for young people of sexting can be very damaging, schools should be clear that such behaviour is not acceptable.

Ofsted specifically refer to sexting in their safeguarding guidance for inspectors, the document states that ‘safeguarding action may be needed to protect children and learners from…the impact of new technologies on sexual behaviour, for example sexting’.

Unfortunately, there is currently no statutory guidance for schools to assist them with dealing with sexting. However, there are a number of other resources available for schools to help them deal with sexting incidents. The Safer Internet Centre has produced two infographics on responding to and managing sexting incidents.

The UK Council for Child Internet Safety (UKCCIS) has produced comprehensive guidance for schools on responding to sexting incidents and safeguarding children. While the guidance is non-statutory, it is endorsed by the DfE, and the NEU was consulted in its production. The NEU advises schools to follow the UKCCIS guidance when dealing with sexting incidents in schools, and when producing school policies on this issue.

Both the UKCCIS and Safer Internet Centre guidance advise that sexting should be dealt with as a safeguarding issue, and any disclosures should be dealt with via the school’s child protection procedures, and in all cases be referred to the designated safeguarding lead.

The response to the incident will depend on its nature, and the UKCCIS guidance states that ‘it won’t always be appropriate to inform the police’. If the child is considered to be at risk, a referral to social services may be necessary. The guidance contains a number of flow charts which can help schools decide on an appropriate response. For instance, if the child is particularly young (i.e. 13 or under), if the images have been distributed without the child’s consent or if there are exploitation concerns, a referral to the police and children’s social care will be required.

All incidents should be recorded by the designated safeguarding lead, even if a decision is made not to refer the case onto any external agencies.

NEU self-help guidance for members addressing sexting incidents in schools is available on the NEU website (Sexting incidents in schools).

The NEU believes that every school should seek to ensure that:

- school governors, head teachers, and senior management team members are familiar with the Government's guidance 'Cyberbullying: Advice for headteachers and school staff' https://www.gov.uk/government/publications/preventing-and-tackling-bullying. Further information on cyberbullying is available from ChildNet.

- 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.

- parents and carers are aware of how to communicate with the school and that it is not acceptable for them to disparage and bully staff via social media sites.

- parents and learners are aware that it is a criminal offence to publish details of any allegation of abuse against a member of school staff on social media if the details published are likely to lead to the identification of the person accused (further NEU guidance addressing allegations of abuse against staff is available at https://neu.org.uk/).

- learners are safe when accessing the internet in school. Schools should consider whether social networking sites with a reputation for cyberbullying should be blocked.

- all staff are provided with information and professional development opportunities to help them understand, prevent and respond to cyberbullying, sexting incidents and other online safety issues and that they are kept up-to-date with developments in technologies that are used by young people. It is particularly important that they understand the child protection and other legal issues that may relate to cyberbullying, sexting and online safety incidents.

- school policy, guidance and information relevant to cyberbullying and online safety is regularly reviewed, to ensure that it meets the needs of pupils and staff. In addition to a specific online safety policy, other relevant school policies should refer to online safety, cyberbullying and sexting. These are likely to include: behaviour policies, safeguarding policies and policies governing the use of mobile and/or smart phones and other portable devices including tablets in schools.

- the reporting routes and relevant responsibilities are made clear. A nominated member of the senior management team should lead on, and oversee, online safety within the school including anti-cyberbullying activity and incidents. Some staff may find it difficult to report instances of cyberbullying to the nominated member of staff, and where this is the case they should feel free to seek advice from their NEU school representative. Sexting incidents should be dealt with as a child protection issue, and all cases should be referred to the school's designated child protection officer.

- the benefits of technology are understood and promoted, whilst at the same time recognising that there are dangers which must be addressed.

- learners support each other and are positive in their online communications. Citizenship and PSHE lessons should extol the virtues of using social media positively by highlighting instances where collective action on social media has influenced or changed society for the better.

- the impact of prevention and response policies and practice is monitored annually. Staff, pupils and parents should feel confident that their school effectively supports those who are cyberbullied.

School employees should expect that:

- all incidents that they report will be recorded.

- the school will respond to an incident in a timely and appropriate manner, 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 the school's communications network will be provided to them – this should include guidance about how school devices issued to staff can and cannot be used both on and off the school premises.

- 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.

- where appropriate, the school will contact the police or external agencies.

If a member of school staff is not satisfied with the way in which an incident has been dealt with, they should seek advice from the NEU Adviceline at 0345 811 811, NEU Cymru at 029 2046 5000 or NEU Northern Ireland on 028 9078 2020.

Appendix 1 to this document is an NEU model policy on online safety. Appendix 2 sets out a list of do's and don'ts for school staff. Appendix 3 contains details of how iPhone users can check if their phone's location settings are set to track their location as staff may prefer to have this feature disabled on their personal or work phones that they use. Appendix 4 contains key points for staff to remember regarding online safety.

Further Information

NEU guidance
Bullying and harassment – health and safety briefing
Cyberbullying – self-help guidance
Sexting - self-help guidance
Social media - self-help guidance
Mobile phone photography - health and safety briefing

DfE guidance - Cyberbullying: Advice for headteachers and school staff

ChildNet guidance - Cyberbullying: Understand, prevent and respond

UKCCIS guidance – Sexting in schools and colleges

NEU MODEL POLICY ON ONLINE SAFETY

Introduction

Staff in schools, as well as children and young people, may be affected by online safety issues including cyberbullying and sexting incidents. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but on their home and work life too. Career progression may be affected, and there have been cases where the person bullied has chosen to leave the education sector altogether. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations. Online safety, however, is about more than cyberbullying. It is about protecting one's online reputation, the managing of personal information and the responsible use of technologies, including social media.

This employer/governing body_________ will ensure that comprehensive online safety education is provided that includes support for both pupils and staff on managing personal information in online environments, and in using personal and social technologies responsibly.

Roles and Responsibilities

This employer/governing body _________ (insert as appropriate) will ensure that this policy will be reviewed and monitored periodically.

The head teacher ________ will ensure that the school has a nominated person as online safety lead (a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of online safety incidents).

All staff will familiarise themselves with this online safety policy and procedures.

Staff e-mails that are marked 'personal' and/or 'union business' will not be read by school management without prior consent.

Responding to cyberbullying incidents and reporting

- Staff should never personally engage with cyberbullying incidents. Where appropriate, they should report incidents to the nominated person and/or seek support.

- Staff should keep any records of the abuse – text, e-mails, voice mail, web site or social media. If appropriate, screen prints of messages or web pages could be taken and time, date and address of site should be recorded.

- Staff should inform the nominated person of incidents at the earliest opportunity.

- Where the perpetrator is known to be a current pupil, colleague or parent/carer, the majority of cases will be dealt with most effectively under the relevant school disciplinary procedure.

- Monitoring and confiscation must be appropriate and proportionate. Except in exceptional circumstances (for example, where disclosure would prejudice the conduct of a criminal investigation) parents, employees and learners will be made aware, and their consent sought, in advance of any monitoring (for example, of e-mail or internet use) or the circumstances under which confiscation might take place. Searches without consent can only be carried out on the school premises or, if elsewhere, where the member of staff has lawful control or charge of the pupil, for example on school trips in England or in training settings. The powers only apply in England.

- Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police inquiries.

- Where pupils are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.

- Staff should report all incidents to the nominated person.

Responding to sexting incidents and reporting procedures

- Incidents of sexting, i.e. the production and/or sharing of indecent images and videos of children under the age of 18, will not be tolerated.

- If staff members receive a report of, or suspects, a sexting incident, they should refer the issue to the school's designated safeguarding lead via the school's normal child protection procedures.

- If a device is involved – it should be secured and switched off. Staff should not search the device if this will cause further embarrassment/distress to the pupil involved, unless there is clear evidence to suggest there is an immediate problem.

- The safeguarding lead must treat all sexting incidents as a child protection issue, and apply judgement, in a consistent manner, to decide on a response to each case. Further advice on issues to consider when making a judgement is available here.

- A risk assessment should be carried out, and necessary safeguards put in place for the pupil (e.g. they might require counselling or further support).

- Sanctions will be enforced if any member/s of the school community breaches school policies relating to sexting. If the images are considered illegal, this may involve making referrals to the police. It there are concerns that the child is at risk, a referral to children's social care is likely to be necessary.

- All sexting incidents must be recorded by the school's designated safeguarding lead, regardless of whether the incident leads to a referral to external agencies.

Action by school: Inappropriate use of social media

Following a report of inappropriate use of social media, the nominated person will take the following action:

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.

- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed.

- In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

- Before the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

Where the alleged 'offender' is a member of the school community (including parents/carers) the school will:

- deal with harassment and bullying under the relevant school procedure;

- take care to make an informed evaluation of the severity of the incident;

- deliver appropriate and consistent sanctions; and

- provide full support to the staff member(s) affected.

The employer/governing body _____________ (insert as appropriate) recognises its legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.

In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff, and parents where necessary.

APPENDIX 1

USEFUL INFORMATION FOR NOMINATED ONLINE SAFETY LEADS

Useful information for the nominated online safety lead including a list of service providers is set out below.

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. They can help you to change the number of the person being bullied if necessary. It is not always possible for operators to block particular numbers from contacting the person being bullied, but many phones, such as iPhone allow users to block phone numbers.

If the victim wants the perpetrator prosecuted contact the police. If a bully is making direct threats which constitute a real danger, phone 999. If there isn't an immediate danger, then contact the non-emergency number 101. The mobile provider can work closely with the police and can usually trace malicious calls for them.

Contact details for service providers:

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Contact details for social networking sites:

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. Advice can be found here.

Facebook	YouTube
Read Facebook's rules	Read YouTube's rules
Report to Facebook	Report to YouTube
Facebook Safety Centre	YouTube Safety Centre

Instagram Read Instagram's rules Report to Instagram Instagram Safety Centre	**Twitter** Read Twitter's rules Reporting to Twitter
Vine Read Vine's rules Contacting Vine and reporting	**Kik Messenger** Read Kik's rules Reporting to Kik Kik Help Centre
Ask.fm Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.	**Tumblr** Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email
Kiwi Read Kiwi's rules Report to Kiwi	

Video and photo hosting sites

YouTube: Logged in YouTube members can report inappropriate content here.

Flickr: Reports can be made via the `Report Abuse' link which appears at the bottom of each page. Logged in members can use the `flag this photo' link to report individual pictures.

Instant Messenger

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their services. Instant Messenger providers can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations and most IM providers allow the user to record all messages.

Contacts details for some IM providers:

WhatsApp: There are details in the FAQs section on blocking other users. There isn't a service to report abuse, but details can be emailed to support@whatsapp.com.

Snap Chat: safety information and reporting options are available here.

Skype: advice on reporting abuse.

Chatrooms, individual website owners/forums, message board hosts

It is good practice for chatroom providers to have a clear and prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

Live streaming

You Now: safety information and details of how to contact a moderator available here.

Periscope: details of how to report inappropriate content are available here and the terms of service are available here.

APPENDIX 2

How to stay 'Cybersafe' – Do's and don'ts for school staff

Do

- be aware of your on-line reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available on-line information. Type your name into various search engines to see what information there is about you on the internet. Remember, the internet never forgets!

- keep passwords secret and protect access to accounts – always log off from any device that you have been using, even if you are only stepping out of the room for a moment and ensure that all phones and tablets are secured with a passcode or fingerprint recognition;

- regularly review your privacy settings on social media sites and your devices (mobile phone, tablet, laptop etc.);

- discuss expectations with friends and family – are you happy to be tagged in photos?

- be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites;

- keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents;

- use a school mobile phone when on a school trip;

- keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible (Note: you can find out your IMEI number by typing *#06# on your handset – the number will be displayed on the screen);

- ensure that school rules regarding the use of technologies are consistently enforced;

- report any incident to the appropriate member of staff in a timely manner;

- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material (staff need to be aware that taking a screenshot of content which is potentially illegal could result in staff committing a criminal offence) including the URL or web address.

- use your school e-mail and devices only for work purposes.

- be aware that if you access any personal web-based e-mail accounts via the school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance.

- request assurances from management that any e-mails marked 'personal' and/or 'union business' will not be read without your prior consent.

- raise genuine concerns about your school or certain members of staff using your employer's whistle blowing or grievance procedure.

Don’t

- post information and photos about yourself, or school-related matters, publicly that you wouldn’t want employers, colleagues, pupils or parents to see;

- befriend pupils or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents or ex-pupils).

- personally retaliate to any incident, bullying messages;

- criticise your school, pupils or pupils’ parents online.

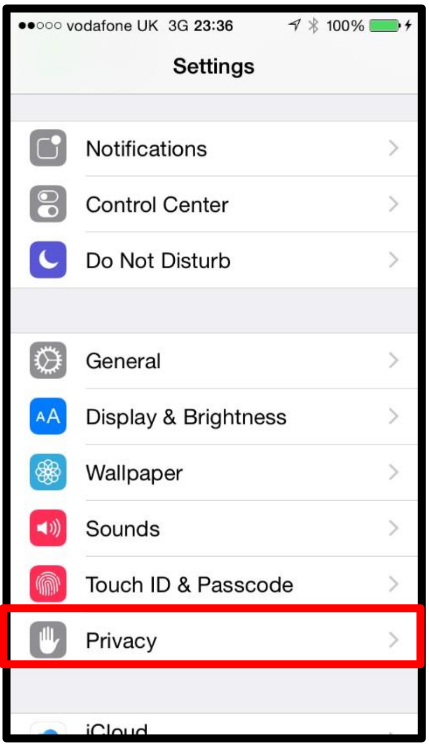
More helpful tips are available from the UK Safer Internet Centre.

APPENDIX 3 – Is my location being tracked?

Is my location being tracked?

Many of us use devices which know where we are, but do we know exactly what information is being collected and why? This tip-sheet addresses one setting on iPhone – frequent locations….

Go to settings and click on Privacy



●●○○○ vodafone UK 3G 23:36 100%

Settings

Notifications >

Control Center >

Do Not Disturb >

General >

Display & Brightness >

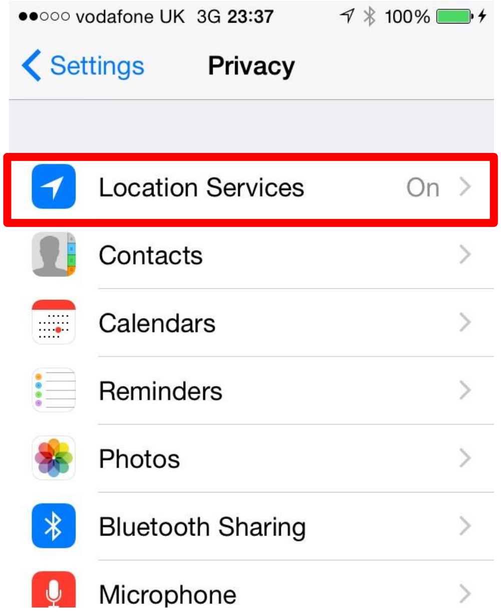
Wallpaper >

Sounds >

Touch ID & Passcode >

Privacy >

iCloud



●●○○○ vodafone UK 3G 23:37 100%

< Settings Privacy

Location Services On >

Contacts >

Calendars >

Reminders >

Photos >

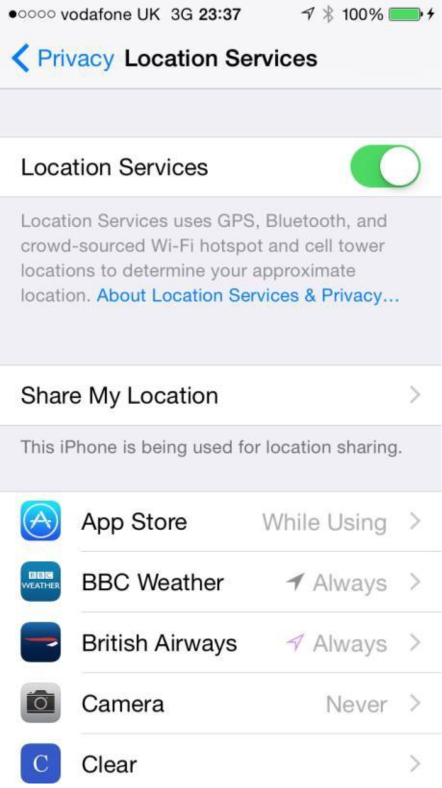
Bluetooth Sharing >

Microphone >

You will see a list of different apps and processes where you can set or alter privacy settings.

Click on Location Services.

You will usually find that location services are enabled (see below) because there are various apps that need to know your location such as weather, maps, social networking services. You may wish to stop some of these apps from being able to access your location.



●○○○○ vodafone UK 3G 23:37 100%

< Privacy Location Services

Location Services

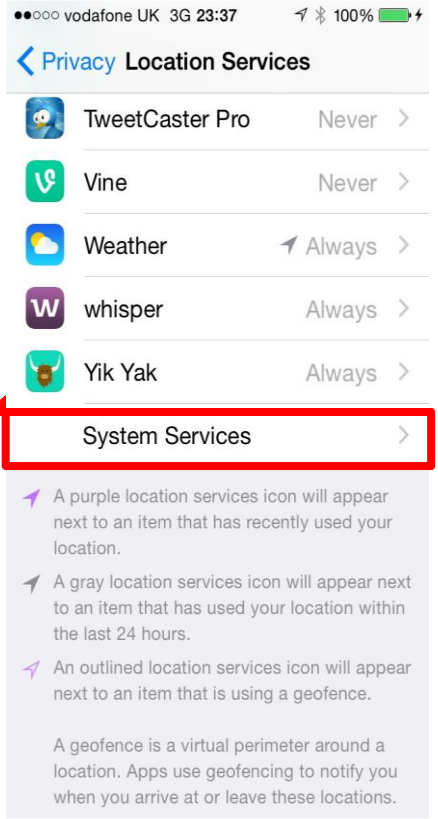
Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy…

Share My Location >

This iPhone is being used for location sharing.

App Store	While Using >
BBC Weather	Always >
British Airways	Always >
Camera	Never >
Clear	>

Scroll down to the bottom of the screen until you can see System Services – click on this.



●●○○○ vodafone UK 3G 23:37 100%

< Privacy Location Services

TweetCaster Pro	Never >
Vine	Never >
Weather	Always >
whisper	Always >
Yik Yak	Always >

System Services >

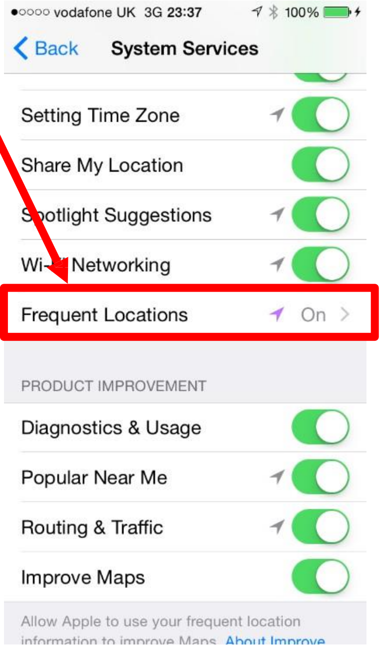
A purple location services icon will appear next to an item that has recently used your location.

A gray location services icon will appear next to an item that has used your location within the last 24 hours.

An outlined location services icon will appear next to an item that is using a geofence.

A geofence is a virtual perimeter around a location. Apps use geofencing to notify you when you arrive at or leave these locations.

Scroll down to Frequent Locations (which you will find at the bottom of the list. You will most probably find that this will be switched on. When you click on frequent locations you will see a list of all of the locations that
you have recently visited. Text here says: *Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.*



●○○○○ vodafone UK 3G 23:37 100%

Back **System Services**

Setting Time Zone

Share My Location

Spotlight Suggestions

Wi-Fi Networking

Frequent Locations On

PRODUCT IMPROVEMENT

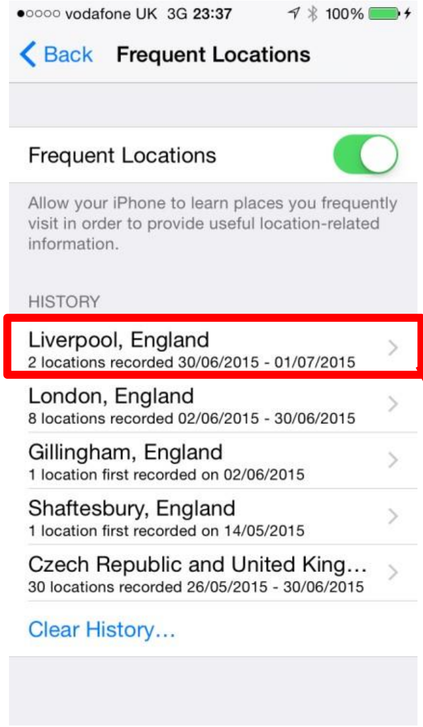
Diagnostics & Usage

Popular Near Me

Routing & Traffic

Improve Maps

Allow Apple to use your frequent location information to improve Maps. About Improve



●○○○○ vodafone UK 3G 23:37 100%

Back **Frequent Locations**

Frequent Locations

Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.

HISTORY

Liverpool, England
2 locations recorded 30/06/2015 - 01/07/2015

London, England
8 locations recorded 02/06/2015 - 30/06/2015

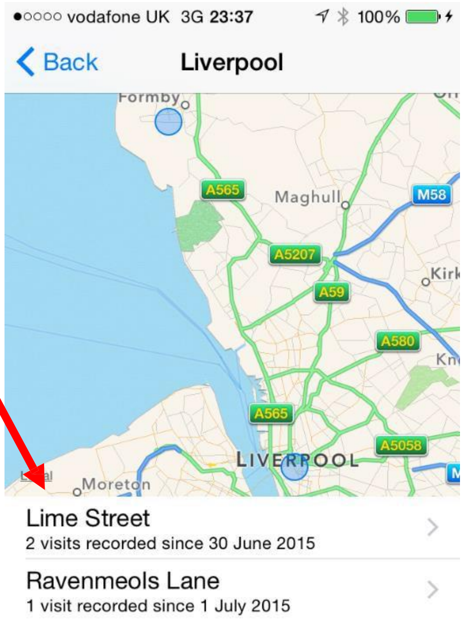
Gillingham, England
1 location first recorded on 02/06/2015

Shaftesbury, England
1 location first recorded on 14/05/2015

Czech Republic and United King…
30 locations recorded 26/05/2015 - 30/06/2015

Clear History…

You will then be able to click on one of these locations to get more information about exactly where it was and when you were there and for how long you were there.



●○○○○ vodafone UK 3G 23:37 100%

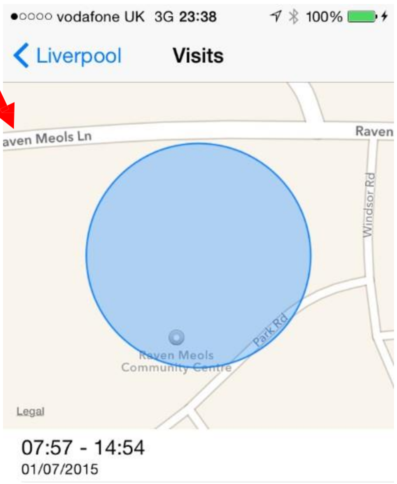
Back **Liverpool**

Lime Street
2 visits recorded since 30 June 2015

Ravenmeols Lane
1 visit recorded since 1 July 2015

Be aware of what you share and if you are not comfortable then take control and make changes.

Further information can be found at
https://support.apple.com/en-gb/HT201357

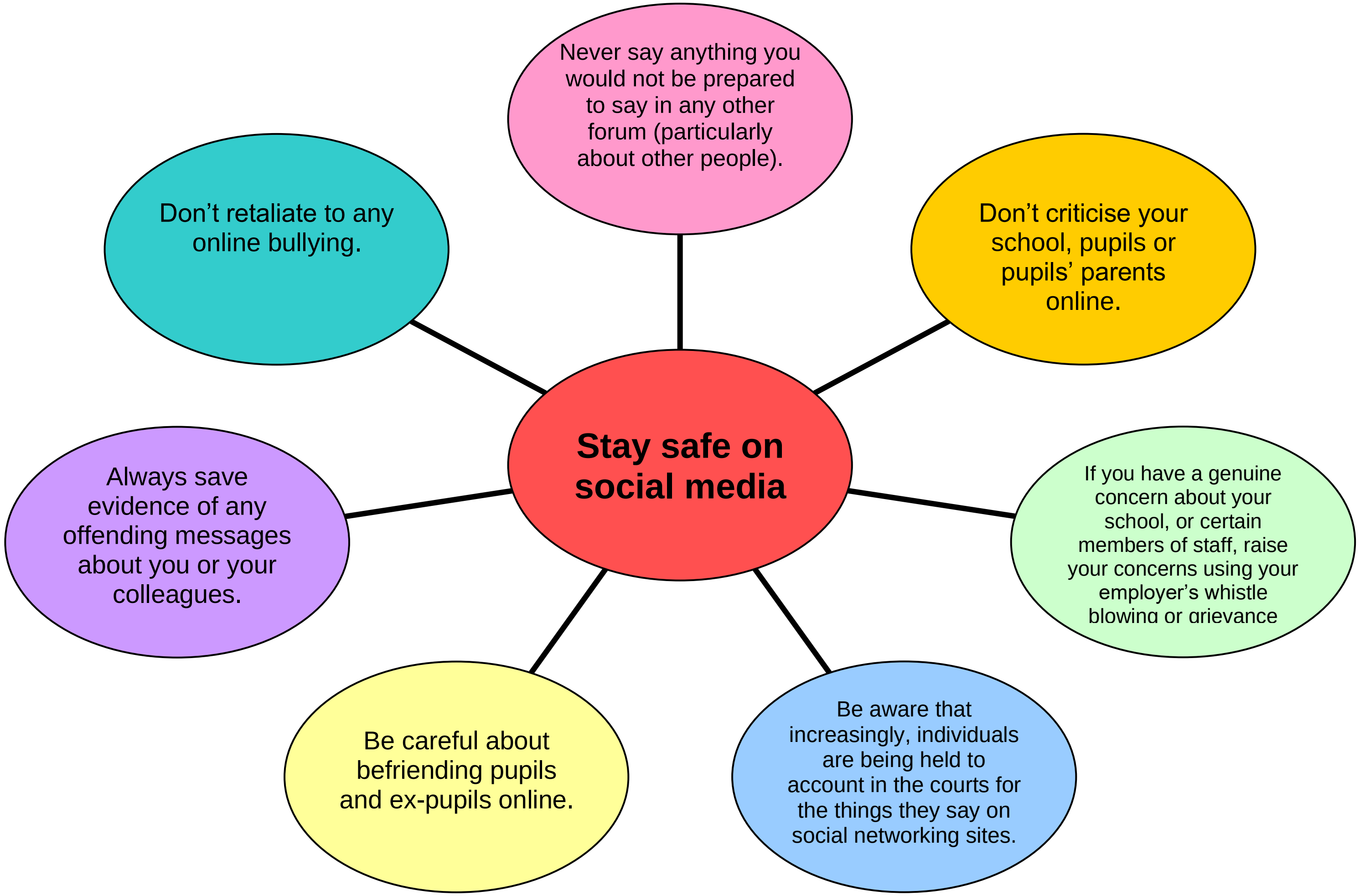


●○○○○ vodafone UK 3G 23:38 100%

Liverpool **Visits**

07:57 - 14:54
01/07/2015

Appendix 4 – Stay safe on social media



Stay safe on social media

Never say anything you would not be prepared to say in any other forum (particularly about other people).

Don’t criticise your school, pupils or pupils’ parents online.

If you have a genuine concern about your school, or certain members of staff, raise your concerns using your employer’s whistle blowing or grievance

Be aware that increasingly, individuals are being held to account in the courts for the things they say on social networking sites.

Be careful about befriending pupils and ex-pupils online.

Always save evidence of any offending messages about you or your colleagues.

Don’t retaliate to any online bullying.