FIVE RIVERS CHILD CARE LTD

Social Media Safeguarding Policy & Procedure – Park House

'Five Rivers is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment'

Policy Owner	Headteacher
Authoriser	Head Of Education
Date of Original Issue	05/06/2020
Date of next review	31/05/2021
Version	V1

Contents

1. Social media and safeguarding policy

1.1 Policy Statement

- Park House School recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.
- Park house school recognises the need for safe use of social media by students at home or in school

1.2 Terms and Definitions

The below table sets out a number of terms and definitions used within this document:

Term	Definition
Nil.	

1.3 Data Protection

- Five Rivers supports the objectives of the General Data Protection Regulation (GDPR) & Data Protection Act 2018 and other legislation relating to Data Processing, including the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Freedom of Information

  Act 2000. Five Rivers Child Care has a statutory obligation to process personal data in accordance with the provisions of the GDPR & Data Protection Act, 2018[1].

- Every member of Five Rivers Child Care has an obligation to ensure that the information they process (use) is collected, maintained and disclosed in accordance with the principles of the GDPR & Data Protection Act, 2018 and the Five Rivers Data Protection Policy.

1.4 Disclosure of Information

- Any use or disclosure of information held within Five Rivers Child Care, without there being a legitimate purpose or legal basis, will comply with the requirements of the GDPR & Data Protection Act, 2018.

1.5 Further Information

2 . Social media safeguarding Policy

2.1 Objectives of the policy

- The purpose of this policy is to encourage good practice, to protect the school , the students and its employees, and to promote the effective use of social media as part of the school activities.
- This policy covers personal and professional use of social media and aims to encourage its safe use by the school , the students and its employees.
- The policy applies regardless of whether the social media is accessed using the school's IT facilities and equipment, or equipment belonging to members of staff or students including equipment supplied for home use to students.
- Personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's reputation are within the scope of this policy.
- Student safety whilst working from home and accessing social media is covered in this policy
- This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.
- Encourage social networking sites to be used in a beneficial and positive way by parents;
- Safeguard pupils, staff and anyone associated with the school from the negative effects of social networking sites;
- Safeguard the reputation of the school from unwarranted abuse on social networking sites;
- Clarify what the school considers to be appropriate and inappropriate use of social networking sites by parents;
- Set out the procedures school will follow where it considers parents have inappropriately or unlawfully used social networking sites to the detriment of the school, its staff or its pupils, and anyone else associated with the Academy;
- •Set out the action the school will consider taking if parents make inappropriate use of social networking sites.

2.2 Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, snapchat, Instagram Twitter, Google+, Instagram, Myspace, Flickr and YouTube.

Social networking sites such as Facebook and Twitter Instagram and snapchat are now widely used. This type of media allows people to communicate in ways that were not previously possible that can positively enhance means of communication. The school recognises that most stakeholders use this in a positive and responsible manner. However, for a minority, such sites can be inappropriately used as a means of expressing negative or offensive views about school and their staff instead of approaching the school where the vast majority of concerns are easily dealt with and resolved. This document sets out the school's approach to parental use of such sites and sets out the procedures we will follow and action we may take when we consider that parents have used such facilities

inappropriately. When we have referred to "parent" in this document, we also include carers; relatives; or anyone associated with the school.

2.3 Roles, responsibilities and procedure

Staff should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer;
- be aware that any excessive use of social media in school may result in disciplinary action;
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the trust, or even future employers, to read. If in doubt, don't post it!
- Not add or `friend` pupils on social media sites or comment on or message a pupil at any time
- 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.

The Headteacher should :

- Have a responsibility to staff ;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'

- addressing any concerns and/or questions employees may have on the use of social media;
- operating within the boundaries of this policy and ensuring that all staff pupils and parents understand the standards of behaviour expected of them.
- Making students and parents of students accessing school equipment at home aware of the safe use of the equipment regarding social media.

The parents/ carers/students should;

Social networking sites have potential to enhance the learning and achievement of pupils and enable parents to access information about school and provide feedback efficiently and easily. In addition, the school recognises that many parents /carers and students and other family members will have personal social networking accounts, which they might use to discuss/share views about school issues with friends and acquaintances. As a guide, individuals should consider the following prior to posting any information on social networking sites about school, its staff, its pupils, or anyone else associated with it:

- Is the social networking site the appropriate channel to raise concerns, give this feedback or express these views?
- Would private and confidential discussions with school be more appropriate? E.g. if there are serious allegations being made/concerns being raised. Social media/internet sites should not be used to name individuals and make abusive comments about those people. Please contact school to discuss any concerns you may have.
- Are such comments likely to cause emotional or reputational harm to individuals which would not be justified, particularly if school has not yet had a chance to investigate a complaint?
- The reputational impact that the posting of such material may have to school; any detrimental harm that the school may suffer as a result of the posting; and the impact that such a posting may have on pupils' learning.

2.4 Acceptable use:

Acceptable/inappropriate use of social networking sites by parents/ carers and students

Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about school (and those associated with it), it is never appropriate to do so. Where a parent/carer/student has a concern, this must be made through the appropriate channels by speaking to the lead teacher, the Headteacher or Head of education so they can be dealt with fairly, appropriately and effectively for all concerned. (See Complaints Policy)

- The school considers the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):
- Making allegations about staff or pupils at school or cyber-bullying;
- Making complaints about the school or staff at Park House school
- Making defamatory statements about school or staff at Park House school;
- Posting negative/offensive comments about specific pupils/staff at Park House School;
- Posting racist comments;
- Posting comments which threaten violence.
- Posting explicit images

Parents/carers should also ensure that their children are not using social networking/internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media. The school will support the parents to understand the dangers so they may be better placed to explain to and support their children.

Acceptable use by staff ·

Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

Employees should not upload any content on to social media sites that:

- is confidential to the school or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- breaches the general data protection act
- is in any other way unlawful.

Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the school social media accounts . Employees should note that the use of social media accounts during lesson time is not permitted.

3. Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- online bullying;
- grooming, exploitation or stalking;
- exposure to inappropriate material or hateful language;
- encouraging violent behaviour, self-harm or risk taking
- sexting.

In order to mitigate these risks, there are steps staff can take to promote safety on line:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos or information comply with existing policies.
- Follow guidelines regarding sexting included in this policy

Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the DSL or deputy in the school.
- Any online concerns should be reported to the DSL or deputy as soon as identified as urgent steps may need to be taken to support the child.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.
-

3.1 Reporting, responding and recording cyberbullying incidents

- Staff and pupils should never engage with cyberbullying incidents. If staff at Park House , discover a website containing inaccurate, inappropriate or inflammatory written material relating to them or images of them which have been taken and/or which are being used without their permission, they should immediately report this to the headteacher or head of education .

- If a pupil or parent /carer of a pupil discover a website containing inaccurate, inappropriate or inflammatory written material relating to them or images of them which have been taken and/or which are being used without their permission, you should immediately report this toa DSL the headteacher or head of education .
- Staff should inform the DSL of incidents at the earliest opportunity.
- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.
- 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 Online safety charge of the pupil, for example on school trips in England or in training settings.
- • 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 following the behaviour policy

3.2 `SEXTING`

'Sexting' is a broad term which can refer to a variety of behaviours, but for the purposes of this guidance , 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.
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'.

The Safer Internet Centre has produced guidance on how to mange incidents of sexting that are contained in appendix 4

The UK Council for Child Internet Safety (UKCCIS) has produced comprehensive guidance for schools on responding to sexting incidents and safeguarding children. Appendix 5.

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.

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 in appendix 1

- 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.

3.3 Action by Headteacher: inappropriate use of social media

- Following a report of inappropriate use of social media, the head teacher will conduct a prompt investigation.
- If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the school's behaviour policy.
- 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 headteacher 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 headteacher contacts a service provider, they 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, they will be clear how it contravenes the site's terms and conditions.

- The Headteacher, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, ie within 24 hours. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.

- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.
- If the material is threatening and/or intimidating, the Headteacher will, with the member of staff's consent, report the matter to the police.
- The member of staff will be offered full support and appropriate stress counselling.

Where the alleged 'offender' is a member of the school community (including parents/carers) the headteacher 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 person(s) affected.

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

4. Breaches of this policy

Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the schools bullying or disciplinary procedure. The member of staff will be expected to co-operate with the school's investigation which may involve:

- handing over relevant passwords and login details;
- printing a copy or obtaining a screenshot of the alleged unacceptable content;
- determining that the responsibility or source of the content was in fact the member of staff.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school or the individuals concerned. Staff should be aware that actions online can be in breach of the school policies including but not limited to sections on harassment/IT/equality .Any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee. Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

5. Monitoring and review

If the Headteacher or head of education reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the school network.

This policy will be reviewed on a yearly basis and, in accordance with the following, on an as-and-when-required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported.

This policy does not form part of any employee's contract of employment and may also, after consultation , be amended from time to time by the school

6. Legislation

Acceptable use of social networking must comply with UK law. In applying this policy, the school/trust will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium. When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment. Staff should use discretion and common sense when engaging in online communication. There are some general rules and best practice in the appendix which staff may find helpful.

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 nonemergency 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.

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

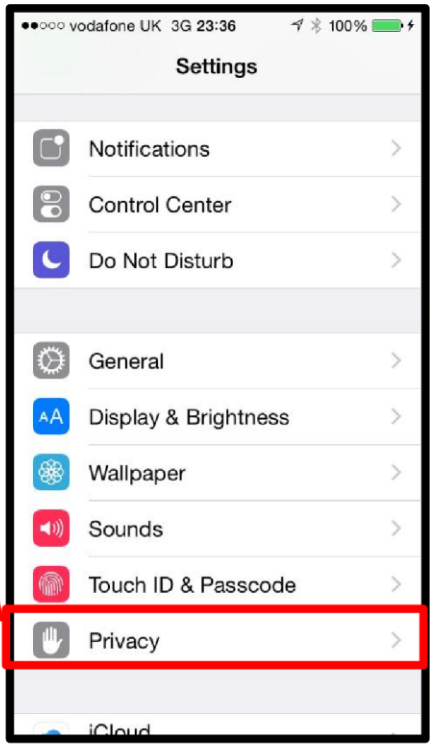
- criticise your school, pupils or pupils' parents online.

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

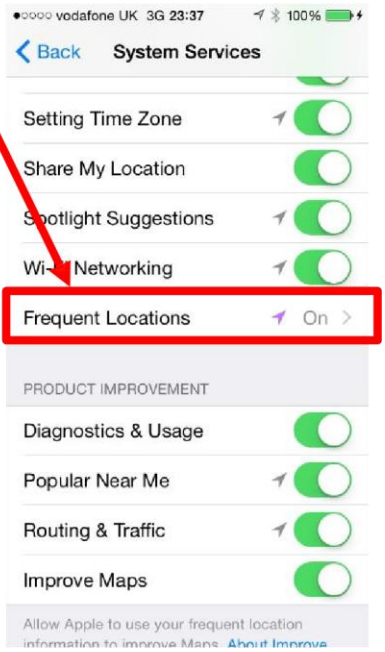
You will see a list of different apps and processes where you can set or alter privacy settings.

Click on Location Services.

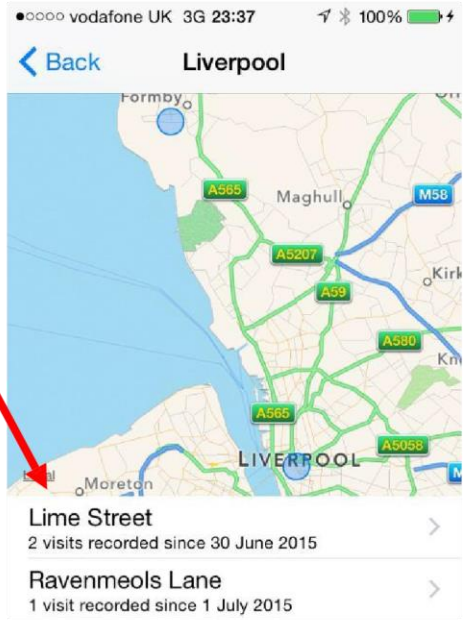
You will usually find that location services are enabled (see below) because there are various apps that need to know your location such as weather, maps, social networking services. You may wish to stop some of these apps from being able to access your location.

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

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.*

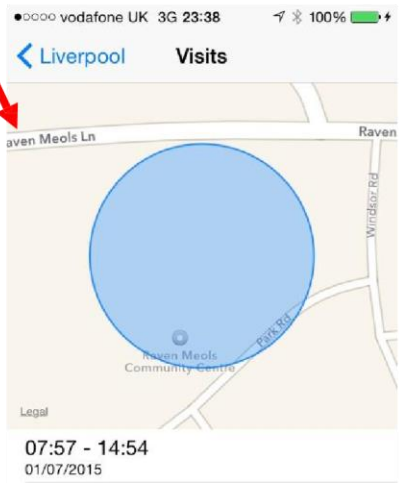


You will then be able to click on one of these locations to get more information about exactly where it was and when you were there and for how long you were there.



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



Appendix 4 – Stay safe on social media

Appendix 5

Advice for schools: Responding to & Managing Sexting Incidents

Context

With the rise of sexting incidents involving young people, this guidance aims to help schools identify sexting incidents, manage them and escalate appropriately.

For School Staff

Remember: The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Step 1:
If a device is involved - confiscate it and set it to flight mode or, if not possible, switch it off.

Step 2:
Seek advice - report to your designated safeguarding lead via your normal child protection procedures.

For the Designated Safeguarding Lead

Record all incidents of sexting, including both the actions you did take as well as the actions you didn't take and give justifications. In applying judgement to each incident, consider the following:

- Is there a significant age difference between the sender/receiver involved?
- Is there any external coercion involved or encouragement beyond the sender/receiver?
- Do you recognise the child as more vulnerable than usual i.e. at risk?
- Is the image of a severe or extreme nature?
- Is the situation isolated or has the image been more widely distributed?
- Have these children been involved in a sexting incident before?
- Are there other circumstances relating to either sender or recipient that may add cause for concern i.e. difficult home circumstances?

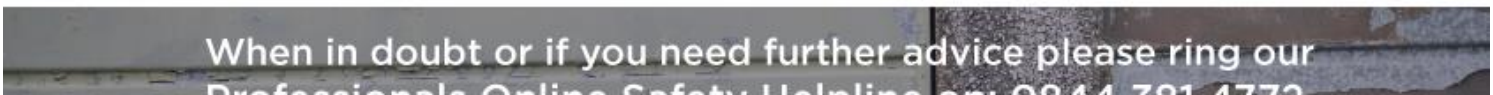
If any of these circumstances are present, then do escalate or refer the incident using your normal child protection procedures. This includes reporting to the police.

If none of these circumstances are present, then manage the situation accordingly within the school and without escalating to external services. Record the details of the incident, action and resolution.

SWGfL Education that Clicks

UK Safer Internet Centre

Co-financed by the European Union
Connecting Europe Facility



When in doubt or if you need further advice please ring our

Appendix 6

Sexting: how to respond to an incident

An overview for all teaching and non-teaching staff in schools and colleges

UK COUNCIL FOR CHILD INTERNET SAFETY

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.

All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.

The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), ***Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People***, and should **not** refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as **the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

2. What to do if an incident involving 'sexting' comes to your attention

Report it to your Designated Safeguarding Lead (DSL) immediately.

- **Never** view, download or share the imagery yourself**,** or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- **Do not** share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies should outline codes of practice to be followed.

3. For further information

Download the full guidance Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016) at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukcci