ONLINE SAFETY POLICY

INTRODUCTION

While new technologies are enhancing communication and creativity some are also challenging the definitions and boundaries of the school environment. As active participants in a digital world our broad curriculum and our pupils' personal goals requires regular use of a variety of IT systems and communication tools. While developments in technology may bring staff and pupils into contact with a wide variety of influences, some of which may be unsuitable, our schools provide a progressive and appropriate education programme for staff, pupils and parents. Our aim is to provide pupils and staff with the knowledge, skills and confidence to become safe and responsible users of technology.

SCOPE

This Online Safety Policy relates to all members of the Thomas's community who have access to, and are users of IT systems and resources both in and out of school and applies to all electronic devices and services provided, whether accessed within school or an external location.

AIMS

The aims of this policy are to ensure that:

- staff and pupils are responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff and pupils are protected from potential risk in their use of ICT in their everyday work
- pupils, staff and parents are aware of the School's expectations and respect the privacy of all members of the school community

The main areas of risk for our school community can be summarised as follows:

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Advertising Spam Copyright Sponsorship Hacking	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading info/advice Body Image and self-esteem Distressing or offensive content

Contact Child as participant	Tracking Harvesting data Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Sexualised bullying (including sexting) Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including "sexting") Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or "Addiction" Plagiarism

ROLES AND RESPONSIBILITIES

All Users

All users are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy. All staff and pupils (including Principals) will sign an Acceptable Use Agreement and be trained in online safety. All users are expected to model safe, responsible and professional behaviours in their own use of technology.

Safeguarding Team

The Safeguarding team responsibilities are outlined in the Safeguarding and Child Protection policy. They will ensure that all staff receive suitable training and development to carry out their responsibilities in a safe and supportive environment. An online safety log will be kept and reviewed regularly by the Safeguarding team. As part of their induction, new staff will be provided with information and guidance regarding the online safety policy.

Digital Lead

The Digital Lead is regularly updated on current online safety issues and legislation, and is aware of the potential for serious child protection concerns. They take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents.

An awareness and commitment to online safety is promoted across the school community by facilitating training and advice for all staff while ensuring online safety education is embedded within the curriculum. The Digital Lead monitors the impact of online safety training and assesses future training needs.

The Digital Lead communicates regularly with Head teachers, SLT, Principals, DSLs and IT support to discuss current issues, review incident logs, adjust filtering and amend operational procedures. They ensure that online safety incidents are logged as a safeguarding incident and that all staff are aware of the procedures that need to be followed in the event of an incident as outlined in our Safeguarding and Child Protection policy.

Parents, carers and extended family

To support families in helping their children use technology safely our schools will seek to provide information and awareness to parents and carers through;

- Reference to relevant resources and websites on the TLP
- Recommended guidance on technology use in letters and bulletins
- Parents evenings
- External speakers
- High profile national events e.g. Safer Internet Day

EXPECTATONS

All users are responsible for using the school IT and communication systems in accordance with the relevant Safeguarding, Behaviour and Acceptable Use Policies.

All staff will supervise and guide pupils carefully when engaged in learning activities involving online technology, and use common-sense strategies in learning resource areas where older pupils have more flexible access. Any misuse will be reported to the Digital Lead/Safeguarding Team in line with the reporting procedures outlined in the Safeguarding policy. (See Appendix 1 for specific sanctions related to technology use.)

All staff are encouraged to take professional, reasonable precautions when working with pupils, previewing websites and resources before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Thomas's London Day Schools Equipment

Staff are responsible for ensuring that any equipment loaned to them by the school, is used primarily to support their professional responsibilities. The IT team keep a list of all members of staff who have use of a work device and will share this with the Designated Safeguarding Lead of each school.

School devices will only be used by pupils during lessons and with permission from the teacher. Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. 'Device-free' signs to this effect are displayed. All users are required to log off or lock the computer/device when they have finished working or are leaving the computer unattended.

This school maintains equipment to ensure Health and Safety is followed. All device use is open to monitoring scrutiny and the Head/ SLT are able to withdraw or restrict authorisation for use at any time, if it is deemed necessary. The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Personal Mobile Devices

All users must follow the expectations outlined in our Acceptable Use Policy and Parental Guidance. Whether in school or at an off-site event, mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

EDUCATIONAL STRATEGIES

As a response to changing attitudes to technology in the classroom, all teachers share collective responsibility for promoting and enhancing digital literacy. All teachers use cloud based software to communicate and set digital tasks for pupils. They use iPad and Netbook technology in the classroom to further embed digital literacy into the wider curriculum, reaching beyond the Computing classroom.

Our schools:

- have a clear, progressive online safety education programme as part of the Computing curriculum and PSHCE curriculum. This aims to build resilience, critical thinking skills and behaviours appropriate to their age and experience;
- plan online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will regularly remind pupils about their responsibilities through the Pupil Acceptable Use Policy and reinforce messages as part of pastoral activities;
- ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology both in and out of school, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Thomas's London Day Schools are committed to providing our staff with regular training and development opportunities. We provide regular CPD content that reflects current educational research and advances in technology. We ensure that staff have regular opportunities to discuss and reflect on current issues as part of structured safeguarding provision.

SECURITY

Passwords

We ensure that all staff and pupils always keep their passwords and pin numbers private. Passwords and pin numbers must be changed at least twice per year and must be authorised via two-step authentication with a personal mobile phone. If a password is compromised the school should be notified immediately.

Digital Images

Parents have given permission for use of digital photographs or video as part of the school's Terms and Conditions unless they have chosen to opt out and informed the school in writing. Each school keeps a list of these children and this is shared with the school photographers. The nominated list holders are

Battersea: Nicola Diggle
Clapham: Helen Stewart-Morgan
Fulham: Emma Beckett
Kensington: Sarah Gill

Members of staff can also opt out of having their image on Social Media and should inform the nominated list holder in writing.

When using social media, for the privacy and protection of all children and adults it is vital to be vigilant and follow the agreed procedures outlined in the Acceptable Use Policy.

If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. This includes uploading digital images to a website or using mobile devices to photograph or film any pupil, parent or member of staff without their consent.

Photographs published on the web do not have full names or personal details attached. We do not use pupils' names when saving images in the file names or in the tags when publishing photos or videos. Photographs published on Twitter are protected with a watermark to avoid screen-grabbing. If specific pupil photos (not group photos) are used in high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.

Individual and class photographs are taken by an in-house school photographer and can be purchased through the Schoolsnaps website which is available on the parents area of the TLP.

Photographs of events and sports fixtures are taken by a freelance photographer known to the school and who follows the schools' Acceptable Use Policy. The photographs are watermarked and can be purchased through Andrew Maltzoff's website which is available on the parents' area of the TLP

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include Principals, parents or younger children as part of their Computing and PSHE schemes of work. They are advised to be very careful about placing any personal photos on any online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information

School Website

The Head, supported by the Principals, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school website complies with statutory DFE requirements. Where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Cloud Based Software

Thomas's London Day Schools provides staff and pupils from Year 3 upwards with cloud based software for their professional and educational use both in school and at home. Pupils and staff are expected to follow the signed Acceptable Use Policy both on and offsite.

Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community. On school devices, pupils are only allowed to upload and publish within school approved 'Cloud' systems.

Internet access, virus protection and filtering

The school network has educational filtered secure broadband connectivity and ensures network health through use of anti-virus software. A progressive filtering system blocks sites that fall into sensitive categories (e.g. adult content, race hate, gambling) and ensures age appropriate access to resources based on educational needs. The Senior IT manager keeps a log of all changes to filtering systems. Any amendments are made in consultation with the Digital Lead.

The wireless network has been secured to appropriate standards suitable for educational use. The network has a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

Network management (user access, backup)

All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards. Our IT Support team:

- use individual, audited log-ins for all users
- use guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- use teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful
- has additional local network monitoring/auditing software installed
- is required to be up-to-date with services and policies
- has daily back-up of school data (admin and curriculum)
- uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- ensures storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.
- does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.

Senior Leaders at each school work in partnership with the IT Support team and the Head to ensure any concerns about the system are communicated so that systems remain robust and protect pupils. There is a clear disaster recovery system in place that includes a secure, remote, off site back up of data.

Requests for information or help should always be directed to IT support via the helpdesk. Requests for the provision of new software or hardware should be made to your Digital lead.

ONLINE COMMUNICATION

References to online communications and social media include software, applications (including those running on mobile devices), email and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, LinkedIn, YouTube, Wikipedia and Instagram. Also included is the use of SMS and instant messaging clients, such as, WhatsApp, Kik, iMessage and Snapchat. Internet/email use is monitored.

Electronic messages are not anonymous and can be tracked and live forever on the Internet. Social Media sites archive content posted, even when deleted from online profiles. Once information is

placed online, the author relinquishes control of it. A teacher should never share information with pupils or parents in ANY environment that they would not willingly or appropriately share in a school or school-related setting or in the community.

Instagram Groups may be set up for any residential trip lasting 5 or more nights. This is designed to give an overview of the trip, not a detailed account. The feeds are monitored closely to ensure that any identifying comments are removed.

Protect Level Communication

'Protect-level' data (sensitive personal information, in particular regarding SEND or safeguarding issues) should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption. Staff use encrypted devices or secure remote access where staff need to access 'protect-level' data off-site.

All Staff

Staff are instructed to always keep professional and private communication separate. Use of email and internet for personal purposes is permitted but any such use must be limited and must not disrupt staff duties.

Staff members who wish to communicate with pupils online may do so only with the approval of Thomas's, using official Thomas's sites and accounts created specifically for this purpose. These sites are managed and controlled by Thomas's administrators. There should be no connection made between any personal accounts and school accounts used for educational purposes. Use of any school approved social networking will adhere to the Acceptable Use Policy.

Teachers are advised that they should use a separate email address just for social networking so that any other contact details are not given away. They should also be aware that they can be vulnerable to unintended misuses for electronic communication. Email, texting and social media encourage casual dialogue and often innocent actions can easily be misconstrued or manipulated. Social networking sites blur the line between work and personal lives and discretion should be used at all times with both parents and colleagues.
Staff are expected to regularly review their privacy settings to ensure that profiles and photographs are not viewable to the general public. **(See Appendices 5 – 7)**.

Pupils

Pupils are taught about social networking, email, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum. All pupils have their own unique username and password which gives them access to the Internet and other services. Pupils' are required to sign and follow our age appropriate Pupil Acceptable Use Policies both at in school and at home.

Parents

To support parents and extended family in helping their children use technology safely parents are reminded about social networking risks and protocols through our Parent/Carer Acceptable Use Guidance and additional communication materials when required.

INCIDENT MANAGEMENT AND REPORTING

All members of the Thomas's community are encouraged to be vigilant and report issues, in the confidence that they will be dealt with quickly and sensitively, through the Behaviour and Safeguarding policies.

Support may be sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues. The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Requests for information or help with equipment and software should always be directed to IT Support via the helpdesk. Requests for teaching support and guidance with online safety issues should be directed to the Digital Lead.

REVIEW AND MONITORING

An annual audit of online behaviour and risks provides a record for monitoring and measuring the impact of our online safety education. This enables us to actively use pupil, staff and parent voice to inform school development and review the impact of online safety and *prevent* training.

Thomas's London Day Schools reserves the right to monitor staff communications in order to:

- establish the existence of facts;
- ascertain compliance with regulatory or self-regulatory procedures;
- monitor standards, which are achieved by persons using the system in the course of their duties and for staff training purposes;
- prevent or detect crime;
- investigate or detect unauthorised use of the school's telecommunications systems;
- ensure the effective operation of the system such as protection against malware, backing up and making routine interceptions, such as forwarding emails to correct destinations;
- gain access to routine business communications, for instance checking voicemail and email when staff are on holiday or sick leave.

There is widespread ownership and strict monitoring of the policy and it has been agreed by the SLT and approved by Principals. All amendments will be disseminated to members of staff and parents.

REFERENCES

This policy has been informed by:

DfE statutory guidance 'Keeping Children Safe in Education (September 2016)

HM Gov Investigatory Powers Act 2016

DfE advice 'The Prevent Duty' (June 2015) from The Counter-Terrorism and Security Act (2015)

NSPCC: 'Younger children and social networking sites: a blind spot' (2013)

HM Gov The School Information (England) (Amendment) Regulations 2012

HM Gov The Education and Inspections Act 2006 and 2011

UK Council for Child Internet Safety (UKCCIS) est 2010
HM Gov Racial and Religious Hatred Act 2006
HM Gov Communications Act 2003
HM Gov Sexual Offences Act 2003
HM Gov The Education Act 2002, Sections 157 and 175
HM Gov Data Protection Act 1998
HM Gov Criminal Justice & Public Order Act 1994
HM Gov Malicious Communications Act 1988
HM Gov Public Order Act 1986
HM Gov Telecommunications Act 1984
HM Gov Computer Misuse Act 1990
HM Gov Obscene Publications Act 1959 and 1964

See also: Anti-bullying Policy, Behaviour Policy, ICT Acceptable Use Policy and Agreements, Safeguarding and Child Protection Policy

This policy will be reviewed annually			
Latest Review: March 2017	By:	Joanna Copland, Vice Principal, Cerys Yardley, Head of Communications, Michael Swart, Senior IT Manager, Digital Leads, Designated Safeguarding Leads	Changes made
Next Review: January 2018	By:	Joanna Copland, Vice Principal, Cerys Yardley, Head of Communications	

Appendix 1: Sanctions for misuse of ICT equipment and technology
Appendix 2: Guidance on internet restrictions
Appendix 3: Guidance on usage of communication devices
Appendix 4: Online Safety Incident Flowchart
Appendix 5: Protecting your privacy on Facebook
Appendix 6: Controlling visibility on Instagram
Appendix 7: Protecting your tweets on Twitter

ONLINE SAFETY POLICY APPENDIX 1

PREP SCHOOL SANCTIONS FOR THE MISUSE OF ICT DEVICES AND TECHNOLOGY

Please note: All incidents must be recorded on the ICT incident log.

These sanctions apply to the misuse of both school equipment and all types of personal devices brought into school (mobile telephones/tablets/interactive watches etc)

A

- Unauthorised access to a website
- Unauthorised use of devices
- Disrespect of school and/or others' ICT resources
- Unauthorised use of email
- Unauthorised use of social networking sites/instant messaging
- Bringing in of any personal electronic device to a classroom without a teacher's permission

Sanction: Referred to Form tutor for school specific school sanctions.

B

- Continued use of devices during lessons after being warned.
- Continued use of non-educational sites during lessons after being warned
- Unauthorised use of staff logins
- Careless use of school and/or others' ICT resources
- Unauthorised use of any personal electronic device to photograph, film or send messages
- Continued unauthorised use of email after being warned
- Continued unauthorised use of social networking sites/instant messaging after being warned
- Continued unauthorised use of any technology to photograph, film or send messages after being warned
- Unauthorised use of filesharing software or downloading files from the Internet
- Sending of any message that is not polite or sensible
- Accidentally corrupting or destroying others' files without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it
- Editing or deleting computers Internet history files

Sanctions: Referred to Form Tutor and Digital Lead. Removal of Internet access rights and/or device for fixed period.

C

- Deliberate damage to school and/or others' ICT resources
- Deliberately corrupting or destroying someone else's files
- Using any ICT device, either in or out of school, to deliberately hurt, upset, bully or harass anyone in the school community
- Deliberately trying to access offensive material
- Deliberately attempting to bypass the school's network security systems
- Using any device to purchase or order items over the Internet

Sanctions: Referred to Digital Lead and Head. Parents contacted. Probable removal of ICT access and or personal device for fixed period.

D

- Continued use of any ICT equipment or devices, either in or out of school, to deliberately hurt, upset, bully or harass anyone in the school community
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic terrorist related or violent
- Using ICT resources to bring the school into disrepute

Sanctions: Referred to Digital Lead and Head. Parents contacted. Probable exclusion for fixed period.

ONLINE SAFETY POLICY APPENDIX 2

INTERNET USAGE RESTRICTIONS

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓
	criminally racist material in UK				✓
	pornography			✓	
	promotion of any kind of discrimination			✓	
	promotion of racial or religious hatred			✓	
	threatening behaviour, including promotion of physical violence or mental harm			✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the Internet				✓	
Online gaming (educational)			✓		
Online gaming (non-educational)				✓	
Online gambling				✓	
Online shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Use of video broadcasting eg Youtube			✓		

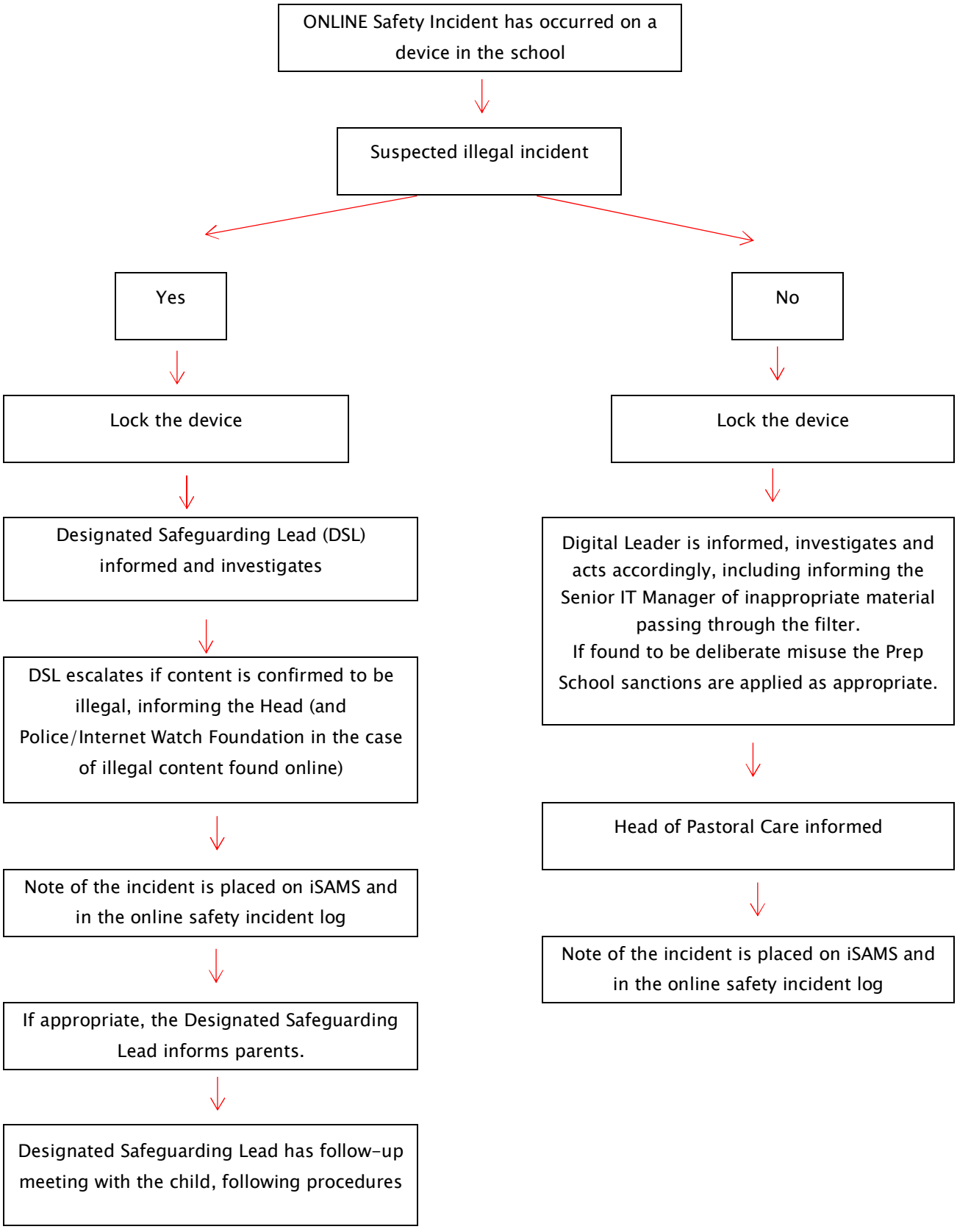
ONLINE SAFETY POLICY APPENDIX 3

COMMUNICATIONS

Communication Technologies that are accepted in school	Staff and other adults				Pupils		
	Allowed	Allowed at certain times	Not allowed		Allowed	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓					✓	
Use of mobile phones in lessons			✓				✓
Use of mobile phones in social time		✓					✓
Taking photos on mobile phones		✓					✓
Taking photos on camera devices	✓					✓	
Use of hand held devices eg PDAs, PSPs		✓				✓	
Use of personal email addresses in school, or on school network		✓				✓	
Use of school email for personal emails			✓			✓	
Use of chat rooms / facilities		✓					✓
Use of instant messaging		✓					✓
Use of social networking sites		✓				✓	
Use of blogs		✓				✓	
Use of forums	✓				✓		

ONLINE SAFETY POLICY APPENDIX 4

ONLINE SAFETY INCIDENT FLOWCHART



ONLINE SAFETY POLICY APPENDIX 5

CONTROLLING YOUR VISIBILITY ON INSTRAGRAM

Setting Your Photos and Videos to Private

How do I set my photos and videos to private so that only approved followers can see them?

By default, anyone can view your profile and posts on Instagram. You can make your posts private so that only followers you approve can see them. If your posts are set to private, only your approved followers will see them in the Photos tab of Search & Explore or on hashtag or location pages. Posts can't be set to private from a desktop computer.

To set your posts to private from the Instagram app:

iPhone or Windows Phone

1. Go to your profile by tapping
2. Tap
3. Turn on the **Private Account** setting

Android

1. Go to your profile by tapping
2. Tap
3. Turn on the **Private Account** setting

Things to keep in mind about private posts:

- Private posts you share to social networks may be visible to the public depending on your privacy settings for those networks. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list.
- Follow requests appear in Activity, where you can approve or ignore them.
- If someone was already following before you set your posts to private and you don't want them to see your posts, you can block them.
- People can send a photo or video directly to you even if they're not following you.

ONLINE SAFETY POLICY APPENDIX 6

PROTECTING YOUR TWEETS ON TWITTER

Protecting and unprotecting your Tweets

When you sign up for Twitter, you can choose to keep your Tweets public or protect your Tweets. Read more about the difference between public and protected Tweets here.

How to protect your Tweets

From the web:

1. Go to your Privacy and safety settings.
2. Scroll down to the **Tweet privacy** section and check the box next to **Protect my Tweets**.
3. Click the **Save** button at the bottom of the page. You will be prompted to enter your password to confirm the change.

From an iOS device:

1. From the **Me** tab, tap the **gear** icon and select **Settings**.
2. Tap **Privacy and content**.
3. Under **Privacy**, and next to **Protect my Tweets**, drag the slider to turn on.

From an Android device:

1. In the top menu, you will either see a **navigation menu** icon or your **profile** icon. Tap whichever icon you have and select **Settings**.
2. Tap **Privacy and content**.
3. Next to **Protect my Tweets**, check the box.

ONLINE SAFETY POLICY APPENDIX 7

PROTECTING YOUR PRIVACY ON FACEBOOK

Facebook's privacy and security settings are frequently subject to change; therefore, staff should regularly check the audience of their profile information and posts (i.e. statuses; uploaded photos; and shared posts).

All Facebook profiles can appear on searches; therefore we have pulled together the following guidance at how else you can maintain your privacy.

1. Restricting who can see your old posts

Desktop: Navigate to "**Privacy Shortcuts**"; via the Settings Tab in the Header.

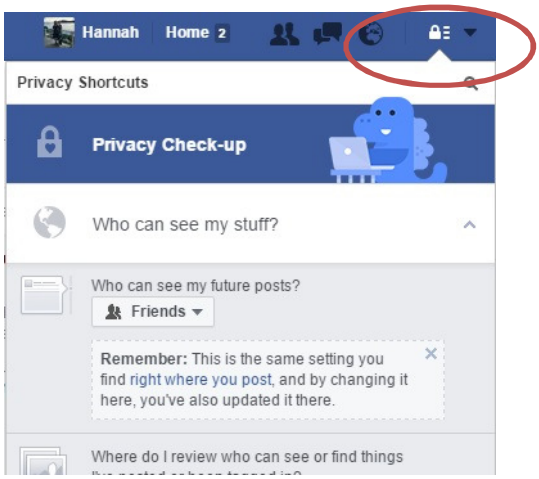
- Click on "**Who can see my stuff**?"
- Click on "**See More Settings**"
- Click on "**Limit Past Posts**" (see attached screenshot)
- You'll see a warning that explains that this tool will limit all of your past posts to an audience of your friends. If there are specific posts that you'd rather be public or visible to friends of friends, you can always go back and adjust them on an individual basis.
- Once you click Limit Old Posts you will get another warning. Click proceed.

Mobile: Navigate to "**Privacy Shortcuts**" accessed directly from your profile or via the Help and Settings Option.

- Click on "**More Settings**"
- Click on "**Privacy**" Click on "**Limit the audience for posts you've shared with friends of friends or Public?**"
- You'll see a warning that explains that this tool will limit all of your past posts to an audience of your friends. If there are specific posts that you'd rather be public or visible to friends of friends, you can always go back and adjust them on an individual basis.
- Once you click Limit Old Posts you will get another warning. Click proceed.

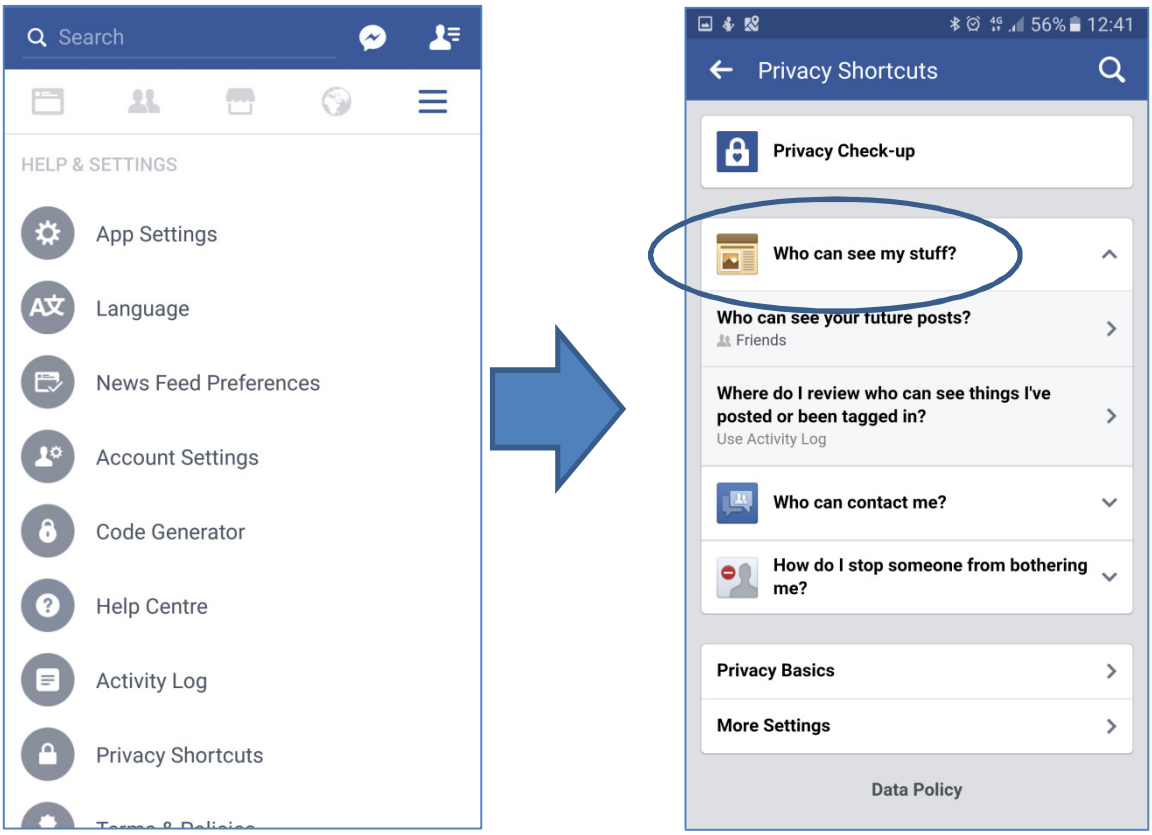
2. Restricting who can see your future posts

Desktop: Navigate to "**Privacy Shortcuts**" via the Settings Tab in the Header.



Click on the drop down **"Who can see my stuff?"**
Click on the dropdown **"Who can see my future posts?"**; and choose **"Friends"**
N.B. This is the same setting you find right where you post; by changing here, you've also updated it there.

***Mobile**:* Navigate to "**Privacy Shortcuts**", accessed directly from your profile or via the Help and Settings Option.
Click on "**Who can see my stuff?**"
Click on **"Who can see your future posts?"**; and choose **"Friends"**



3. Untagging yourself from photos or requesting their removal from Facebook

Click on the photo you have been tagged in, and when the photo opens up, click the ***Options*** button on the toolbar along the bottom.

Then select ***Remove/Report tag*** and you are given the option of simply untagging yourself. This will remove the picture from your profile but it will still exist on Facebook. You can also request that the picture is removed from Facebook completely.

Click on the downward arrow in the top right corner of the screen and select ***Settings*** from the drop down menu.

In the settings menu, under ***Timeline and Tagging***, you can also specify who can see the posts you have been tagged in on your timeline, and the posts that other people have posted on your timeline.

For maximum security, select ***Only me***.

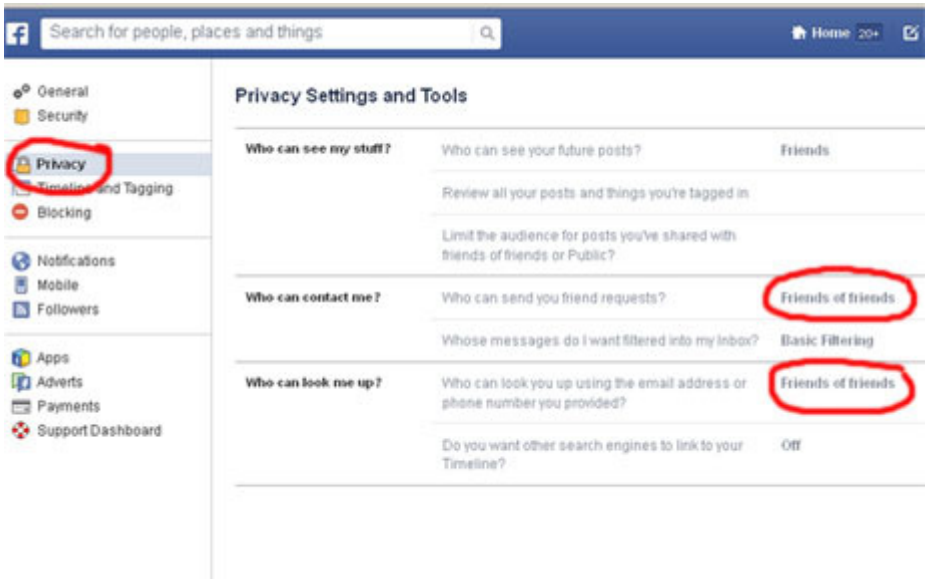
Similarly, you can restrict what certain individuals can see. Click ***Blocking*** in the settings menu and then select ***Edit List*** beside the ***Restricted List*** option.

You can then type in the name of the person and only give them access to the posts and information you make public.

4. How to avoid unwanted friend requests

You can avoid unwanted friend requests by going to your profile and clicking on the downward arrow in the top right corner of the screen.

When the drop-down menu appears, click on ***Settings***, and then when the page refreshes click on the ***Privacy*** option in the left hand menu. Under 'Who can contact me' you can specify who can send you friend requests.



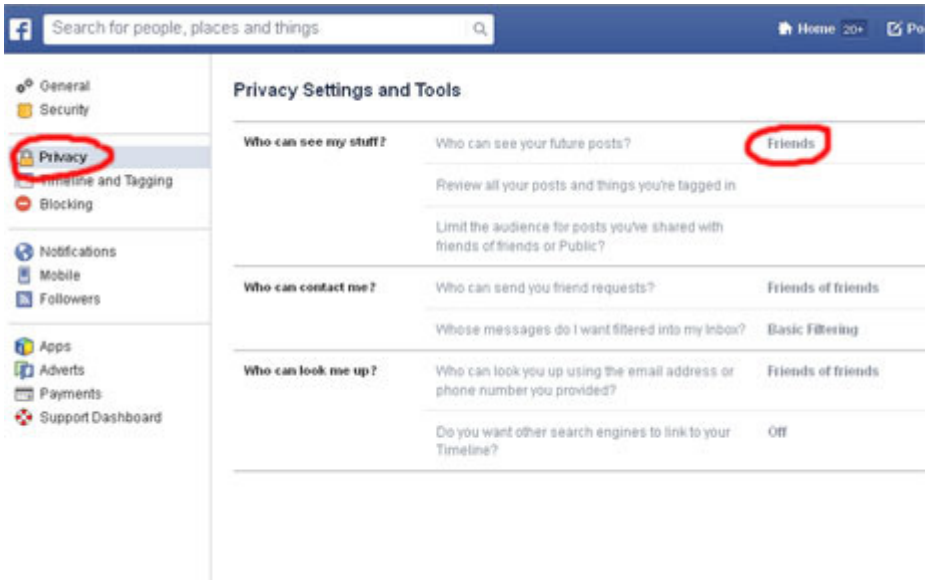
You can also specify who can look you up using your email address or via a search engine. This means that anyone who plugs your name into Google will not get a link to your Facebook profile.

5. Ensuring only Friends can see your profile

Allowing ***Friends of Friends*** to view your profile may seem innocent enough, but it is highly likely that you do not know these people.

Click on the downward arrow in the top right corner of your profile and when the drop-down menu appears, click on ***Settings***.

Then click the ***Privacy*** option in the left hand menu and edit the ***Who can see my stuff?*** option to ***Friends***.



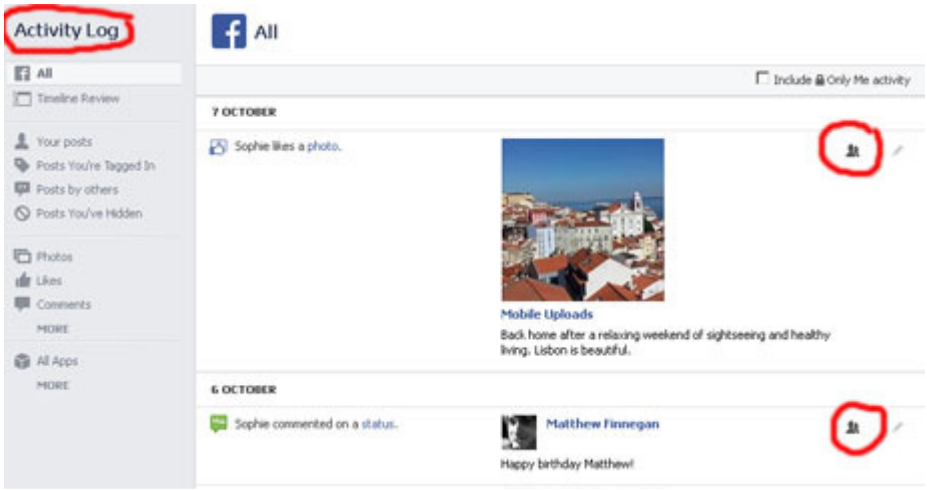
If you receive unwanted or abusive messages from people you don't know, you can make sure any such messages are filtered into your ***Other*** folder via the ***Who can contact me*** setting.

6. Reviewing all your posts individually

It is important to get your Facebook privacy settings right.

Go to the settings on your profile and change ***Who can see my stuff*** to just ***Friends***. Be warned, however, this will only affect your future posts.

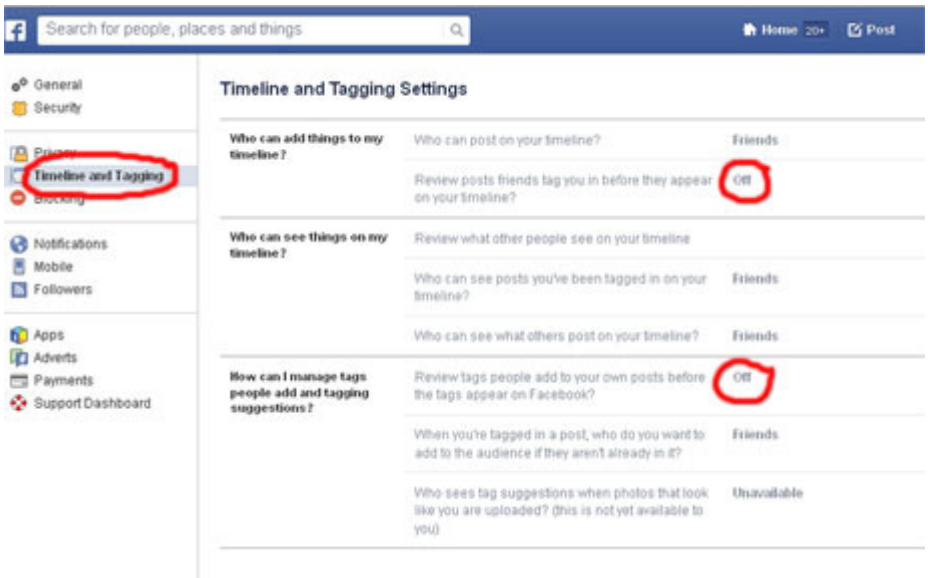
If you want to make older posts or things you have been tagged in invisible, for example to prospective contacts, you need to ***Review all your posts and things you're tagged in***, and use the drop-down menus on the right to limit the audience for each individual post. You can also limit the audience for posts you have shared with friends of friends or in public.



7. Reviewing tagged photos before they go live

In the ***Settings*** menu, select ***Timeline and Tagging***. Here Facebook gives you the option of reviewing posts that friends tag you in before they appear on your timeline.

You can also review tags people add to your own posts before the tags appear on Facebook.



If you want to check what your profile looks like to the general public, or to a certain person, click the ***View As*** link next to ***Review what other people see on your timeline***, and choose the perspective you want at the top. This is a very useful tool to double check the changes you have made.

8. Rejecting unwanted friend requests

Most of us have had a friend request from someone we'd rather not have seeing our profile.

Hitting the ***Ignore*** button will not alert them that their friend request was declined but they will still be able to send you another friend request in the future.

Alternatively you can choose not to respond at all. And you can choose to ***Hide friend request*** so it does not appear in your list of pending friend requests anymore, saving you from being reminded every time you log on.

If you want to remove hidden friend requests at a later date, you can go to the Friend Requests page by clicking the friend requests icon (the silhouettes in the top right hand corner) and then View All.

Then select ***Delete friend request***.

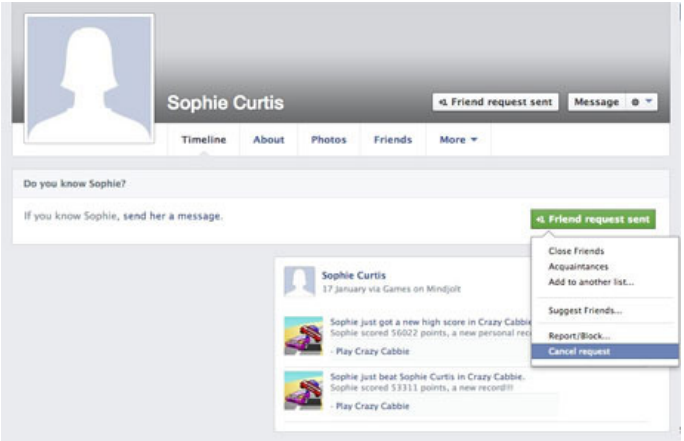
To ensure a total snub without causing offence, you can ***Block*** the person entirely.

This will mean they can no longer see anything you post and will not be able to add you as a friend.

Click the padlock button on the top left of any Facebook page, click ***How do I stop someone bothering me?*** from the drop down menu.

Then enter the name of the person you want to block and then click ***Block***.

If one you have sent a friend request to someone and are having second thoughts or did it by accident, simply select their profile, hover over the ***Friend request sent*** button and select ***Cancel request*** from the drop down menu.



9. Removing location tagging

Facebook can track and publicise where you have been. If you post using your mobile phone then chances are, unless you have turned off location services, it will also tag each post with your location.

Similarly, if friends tag you in a post with a location, it will show up in your timeline.

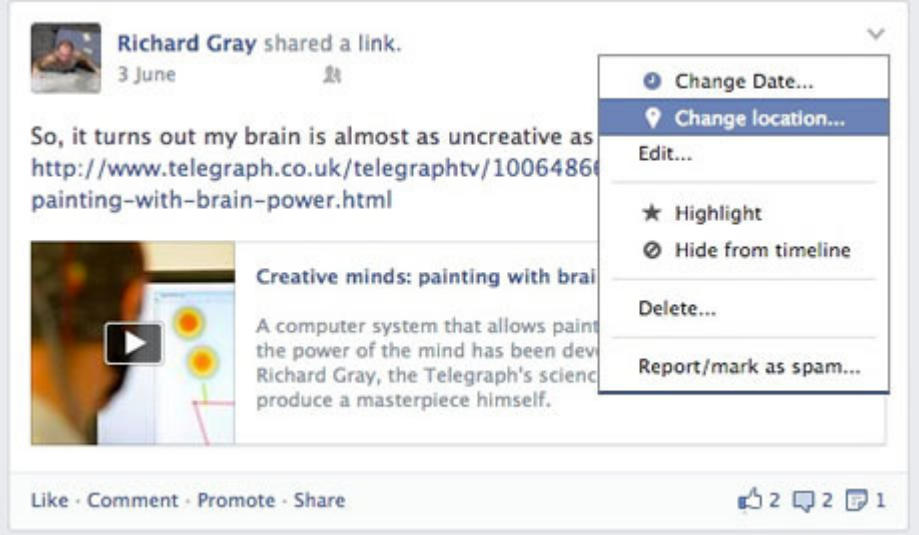
If you have not turned on your security settings, then this information could potentially be exploited by undesirable members of society.

Not only can it reveal where you live from the pictures and posts conveniently tagged, it can also tell the world when you are away.

To prevent posts that you write being tagged with your location, click the little ***x*** beside the location that appears at the bottom of the status update box.

To remove a location after you have posted an update, click the little down arrow that appears in the top right hand corner of the post when you hover over it.

Select ***Change Location*** and then hit the little ***x*** to remove the location and click ***Save***.

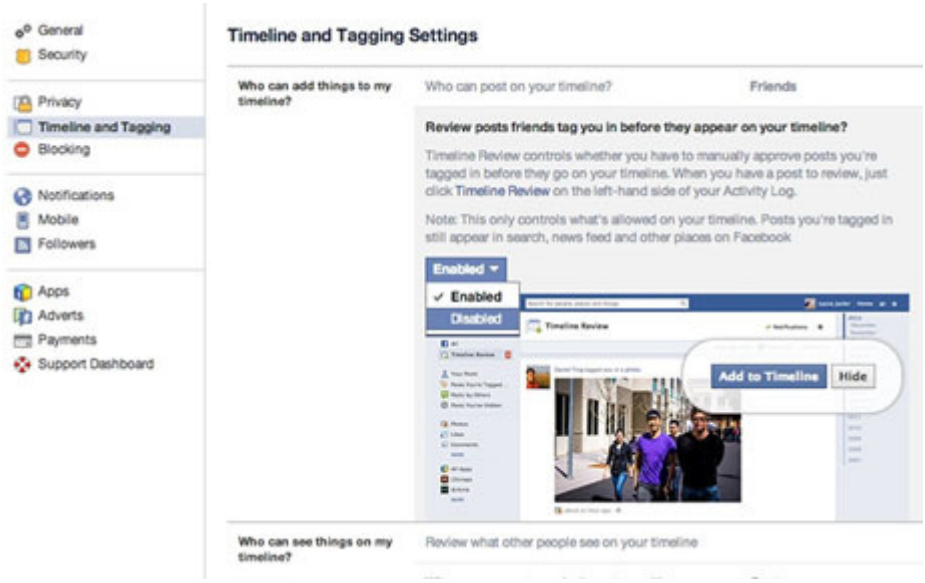


Similarly you can remove your location from posts that friends tag you on.

To prevent friends from revealing your location in tags in the first place, you can set up Facebook to allow you to review every post they make about you.

Turn on ***Timeline review*** by selecting setting the down arrow at the top right of the Facebook page and clicking ***Settings***.

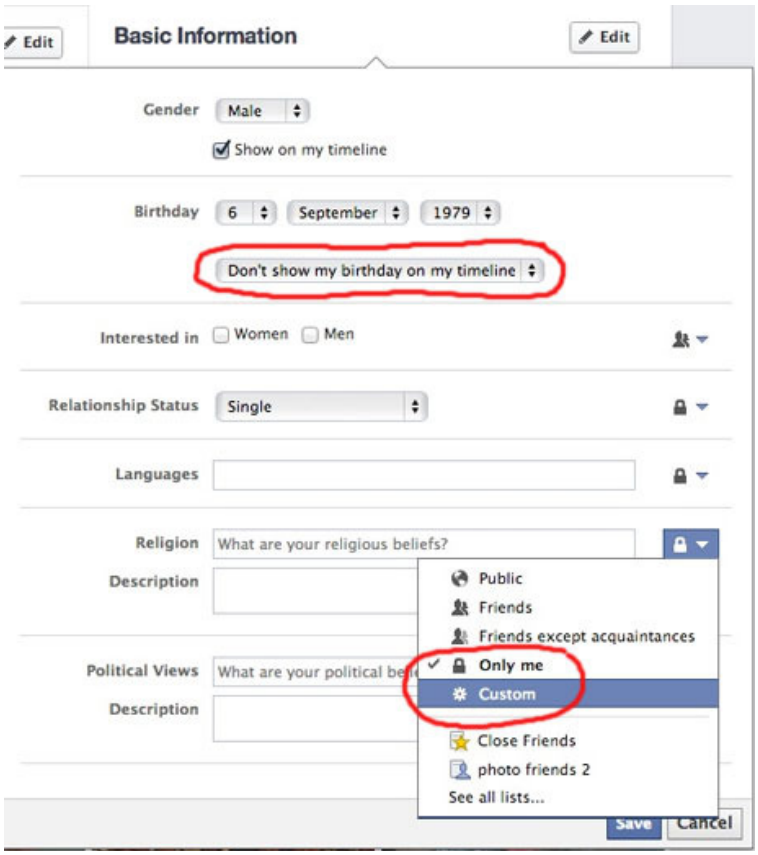
In the left hand column, click ***Timeline and Tagging***. Look for the setting ***Review posts friends tag you in before they appear on your timeline*** and click ***Edit***. Then select ***Enabled***.



10. Changing personal information

If necessary, you can hide some personal information on Facebook. From your profile page, select the ***About*** tag and then click on the ***Edit*** button beside any of the information there you want to keep secret.

For example, if you want to hide your age, click the ***Edit*** button that resides beside ***Basic Information*** and then select ***Don't show my birthday on my timeline*** from the drop down menu under your date of birth.



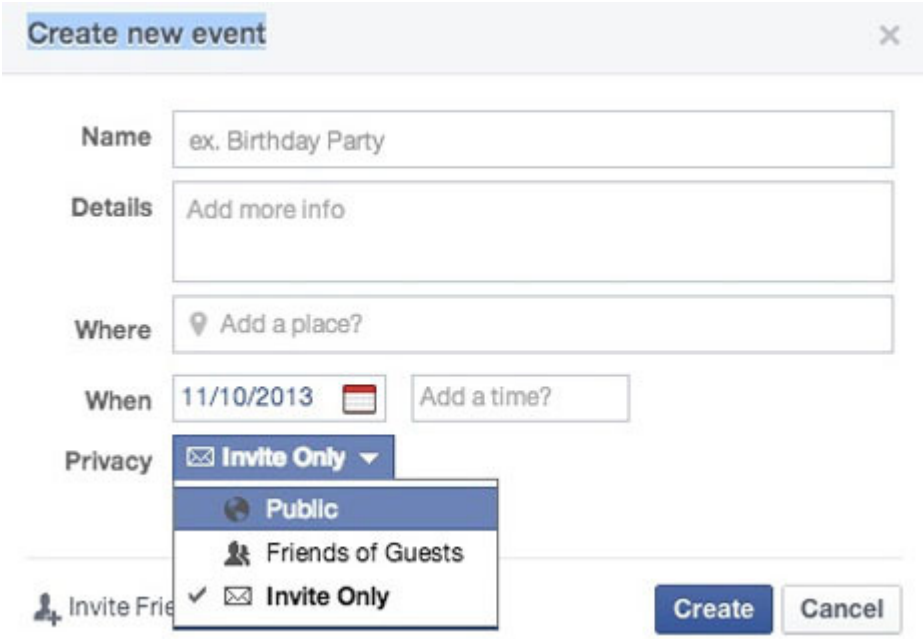
You can also hide your relationship status, gender, your religious beliefs, the languages you speak, your home town and your political views along with any family you may have.

Click on the arrow beside each option and select either ***Only me*** to hide from everyone or ***Custom*** to select a few friends you want to keep secrets from.

11. Making sure events stay private

You can change the privacy of an event when you create it to ensure that unexpected guests do not turn up.

On the ***Event*** page, click ***Edit*** at the top right and then chose a setting from the dropdown menu.



If you select ***Public***, then everyone in the world can see the plans for your particular event.

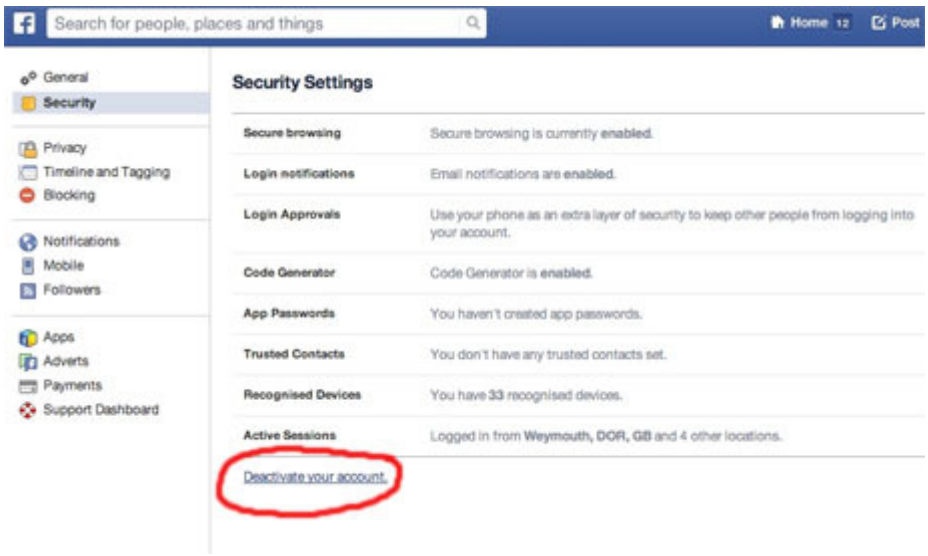
They will also be able to see the videos, photos and posts that go up afterwards.

The safest option is to select ***Invite Only***, then you will be able to type in the names of the people you want to come along and your party will not be visible on any public search results.

12. How to deactivate your account if required

Should you ever wish to leave Facebook you can deactivate your account, which will remove your timeline from the Facebook service. Other Facebook users will not be able to search for you.

To do this click the down arrow at the top right of the Facebook site and choose ***Settings***. Then click ***Security*** from the left-hand column and then ***Deactivate your Account***.



You can reactive your account at any time by logging in with your email and password, restoring your timeline in its entirety.

However, if you want all record of you to be removed, then you can ***permanently deactivate*** your account with no option of it being recovered.

Facebook provide a form that you need to fill in.