NORTHAMPTON SCHOOL FOR GIRLS
E-SAFETY POLICY and CODE OF PRACTICE

Links with other policies:

- ***Safeguarding Children - Child Protection***
- ***Anti bullying***
- ***Behaviour Policy***
- ***Safeguarding Children - Recruitment***
- ***Appropriate Contact with Students***
- ***Health & Safety***
- ***Disciplinary Procedure***

Why have an E-safety Policy?
The use of the Internet as a tool to develop learning, understanding and communication has become an integral part of school and home life. There are always going to be risks in using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children and staff use these technologies. Whilst the school acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to our policy to ensure students are continued to be protected.

Aims
- To outline the roles and responsibilities of staff, students and parents.
- To ensure the safeguarding of all students within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To ensure all users are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- This policy aims to inform how parents/carers and students are part of the procedures and how students are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'E-Safety' is used to encompass the safe use of all on-line technologies in order to protect students and adults from potential and known risks.

Roles and responsibilities of the school
It is important to emphasise that we are **all** responsible for E-Safety and our specific responsibilities are outlined below:

Governors and Co-Co-Headteacher
- It is their overall responsibility to ensure that there is an overview of E-Safety (as part of the wider remit of Safeguarding Child Protection) across the school and that they promote and report on E-Safety developments and their links with the school development plan/ICT development plan, safeguarding child protection, and other policy changes.
- The Governing Body should appoint an E-Safety governor who will challenge the school about having appropriate policies, procedures, staffing responsibilities and ICT security systems.
- The Co-Co-Headteacher should assign the role of E-Safety officer to a member of the senior leadership team.

E-Safety officer - Paul Parker – Assistant Head
It is their responsibility to
- Implement agreed policies, procedures, staff training, and curriculum requirements and take the lead responsibility for ensuring E-Safety is addressed in order to establish a safe ICT learning environment.
- Ensure that the E-Safety Policy is reviewed annually, with up-to-date information available for all staff to teach E-Safety and for parents to feel informed and know where to go for advice.
- Ensure that all adults in the school and parents are aware of the filtering levels and why they are there to protect students.
- Ensure that the filtering levels on all equipment are appropriate for our students and are set at the correct level to ensure that any concerns are reported to him and update the Co-Headteacher regularly
- Keep a log of incidents for analysis to help inform future development and as part of the school's safeguarding procedures

- Ensure there is appropriate anti-virus software and anti spy software in place on all school equipment and that this is reviewed and updated on a regular basis
- Report accidental access to inappropriate materials to the ICT technical manager of the ISP and or filtering service so that inappropriate sites are added to the restricted list
- Responsible for the transparent monitoring of the Internet and on-line technologies. For example- any student or staff files may be accessed if it appears that the E-Safety policy may have been breached on the authorisation of the E-Safety leader or the Co-Co-Headteacher or, if it involves one of the Co-Co-Headteachers, the Chair of Governors.

All staff

- Should have signed that they have read, understood and agreed with the E-Safety staff Code of Practice, (see Appendix I). By signing this agreement they will know that by following the rules they are safeguarded from allegations and that they understand their responsibilities to safeguard students when using on-line technologies.
- They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- When accessing the school system from home, the same Code of Practice will apply.
- Staff should request training or access internal training so that they are updated on new and emerging technologies and are up-to-date with E-Safety knowledge that is appropriate for the age group they teach and reinforce it through their curriculum.
- Ensure the correct procedure is used for dealing with any issues arising from indecent or pornographic/child abuse images sent/received (see Appendix II)
- Ensure that students are protected and supported in their use of on-line technologies and are taught to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- To work closely with tutors and pastoral leaders regarding PSHE so that students are taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.
- Staff are expected to be aware of and adhere to data protection rules when communicating by email and the age appropriateness and legalities of the resources they use and upload to e- learning platforms.
- They must report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies to the Co-Headteacher and on the Northamptonshire County Council accident/incident reporting forms, in the same way as for other non-physical assaults.

Students' responsibilities

- Students are involved in the review of E-Safety policy, the e safety page of the website and the student code of conduct through student voice, the student council and through PSHE programmes of study.
- Students will fully participate in the E-Safety curriculum provided in ICT and PSHE lessons.
- Students are expected to use the Internet and other ICT e.g. mobile phones, digital cameras, webcams, in a safe and responsible manner at all times in school and any other settings including at home.
- Students are responsible for following the E-Safety code of conduct for students whilst within school as agreed at the beginning of Year 7 or whenever a new child attends the NSG for the first time.
- Students are taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, and will be expected to do so knowing that they will not be reprimanded for behaviour which is not their responsibility.

Parents / carers

- All parents and carers are given a copy of the student version of this policy and mission statement on entry to school as part of the 'Useful policies for parents/carers' booklet.
- Parents / carers and students are asked to read and sign the E-Safety code of practice to say they have read the policy and understand the implications for students if there should be any misuse of technologies.
- Are encouraged to seek advice and support from the school via the E-Safety page on our website or by appointment with appropriate staff
- Parents/carers are encouraged to add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.
- Parents are required to support the school in promoting safe use of the internet at home,at school and within the family under the Home School Agreement.

In the event of inappropriate use by Students
When considering any sanction regarding the misuse of technology each case is looked at individually and according to the levels of severity a range of sanctions are considered.

Level 1: Any student found to be misusing the Internet by not following the Acceptable Use Rules will have an E-Safety incident sheet completed by the staff member observing the breach of the rules and a copy sent to the E-Safety officer - depending on the severity of the breach it might lead to level 2 or 3 below.

Level 2: parents/carers will be informed by letter outlining the breaches to the Code of Practice and any consequences such as removal of access to the internet. Appendix II.

Level 3: Following any further breaches parents/carers will be invited into school to discuss their daughter's/ son's online activity. We will see how we can support them through training. For example we will refer to guidance from Child Exploitation and Online Protection (CEOP). It is likely that after this meeting internet access will be restored and students will be asked to sign another copy of the Code of Practice.

In the event that a student accidentally accesses inappropriate materials the student will report this to an adult immediately who should take appropriate action to hide the screen or close the window, and they should then complete an E-Safety incident sheet and a copy sent to the E-Safety officer who will ensure no further access to this site occurs through updating the filtering service. Appendix II

In the event of inappropriate use by Staff
If a member of staff is believed to misuse the Internet or E-learning platforms in an abusive or illegal manner, it will be reported to the Co-Headteacher immediately. We then follow our child protection policy. Appendix II.

E-Safety in the curriculum
We teach our students how to use the Internet safely and responsibly for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning. This will be done in all lessons using ICT and particularly through ICT and/or PSHE lessons so that the following concepts, skills and competencies are taught and revisited as needed. *(For further details see ICT and PSHE schemes of work available on NSGonline)*

Use of email
- We have individual email addresses for students - used as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.
- Staff are to use their school issued email addresses for any communication between home and school only. Students are encouraged to use their school email to contact staff about teaching and learning related issues only. Parents/carers are encouraged to be involved with the monitoring of emails sent although the best approach with students is to communicate about who they may be talking to and assess risks together.

Filtering, Monitoring & Security Systems
We use a combination of hardware and software tools to keep users and computers safe. Which include the following . . . .

- A Meraki MX400:A feature-rich unified threat management system.This appliance includes intrusion prevention, Antivirus and anti phishing filtering.
- Impero Software: Used for the monitoring of users internet access & websites visited. It also analyses keystrokes made and automatically screenshots questionable activity which are forwarded to the heads of year for actioning or escalating as appropriate.
- Eset Anti-virus software is installed on all Servers, Workstations and School Laptops.
- WPA2-PSK & 802.1X with custom RADIUS Encryption is used to access the wireless network.
- A guest SSID is available for guests.
- All users are required to log on to workstations with their school username and password to access any network or internet resource. This then identifies the user on the system.

- NSG requests that users only use the school's email system to communicate with each other. We can trace and recall all emails sent / received should it be required for further investigation. This will be conducted in conjunction with the E-Safety officer.
- Gmail screens all Student emails for profanity. Any email which includes a profanity (from our extensive but not definitive list of banned words) automatically gets deleted and never reaches the intended recipient(s). The sender gets an email which says "your email has been rejected on the grounds that it contravenes the school's "Acceptable Usage Policy"
- All school laptops are encrypted and staff are asked to use a cloud based storage facility where possible. If they use portable storage devices, ie usb sticks or portable hard drives we recommend it is encrypted.
- If a user tries to access a blocked site they will get a message similar to *"This website is blocked by your network operator"* *URL:* *http://bett365.com/*
  Category: *Gambling*
  Server: *204.74.99.100:80*

- Any attempt to access a blocked URL is logged in the Event log example below . . .

  url https://www.facebook.com/..., category0 Social Networking, server 31.13.90.36:443, user Lxxxx Wxxxxx@NSG.local, group Students

We test the filtering system at least half termly and react immediately to any staff or student observations / concerns. Filtering is applied as follows:

Category	SLT/Admin	Staff	Student/Thin Client
Adult and Pornography	✓	✓	✓
Bot Nets	✓	✓	✓
Confirmed SPAM Sources	✓	✓	✓
Gross	✓	✓	✓
Hacking	✓	✓	✓
Hate and Racism	✓	✓	✓
Illegal	✓	✓	✓
Malware Sites	✓	✓	✓
Marijuana	✓	✓	✓
Nudity	✓	✓	✓
Pay to Surf	✓	✓	✓
Peer to Peer	✓	✓	✓
Phishing and Other Frauds	✓	✓	✓
Proxy Avoidance and Anonymizers	✓	✓	✓
Questionable	✓	✓	✓
SPAM URLs	✓	✓	✓
Spyware and Adware	✓	✓	✓
Violence	✓	✓	✓
Weapons	✓	✓	✓
Keyloggers and Monitoring		✓	✓
Unconfirmed SPAM Sources		✓	✓
Alcohol and Tobacco			✓
Auctions			✓
Cheating (Academic)			✓
Cult and Occult			✓
Dating			✓
Gambling			✓
Games			✓
Hunting and Fishing			✓
Individual Stock Advice and Tools			✓
Internet Communications			✓
Personal sites and Blogs			✓
Search Engines			✓
Social Networking			✓
Swimsuits & Intimate Apparel			✓
Web Advertisements			✓
Parked Domains			✓
Abortion			
Abused Drugs			
Computer and Internet Info			

We regularly review our internet monitoring, filtering and security systems in line with national safeguarding guidelines.

Mobiles and Smartphones

- The use of mobiles in school follows the school behaviour policy. Mobile phones may not be used in school except by Sixth Form students who may use them out of lesson time in the Sixth Form Centre ONLY. Any misuse of mobile phones or other technologies will be dealt with according to the guidance of this policy and other related policies e.g. Behaviour policy, Anti-bullying policy.
- Staff members are not allowed to use their personal telephones to contact students, except in emergency if on an off-site visit. They should not store students' numbers on their own phone – this includes students who have left the school in the last three years. If staff have any students' numbers held on personal telephones they must inform the Co-Headteacher of the numbers and the reason for holding them.

Photos & video

- Photographs and video images should only be recorded and / or uploaded on the approval of a member of staff or parent/carer and should not allow individual safety or privacy to be compromised (staff or student) , it should only contain something that would also be acceptable in school. Parents/carers should monitor the content of photographs / videos uploaded at home.
- Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website.
- Photographs should only ever include the child's first name although Child Safeguarding Guidance states either a child's name or a photograph but not both.
- Group photographs are preferable to individual students and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.
- The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission must always be sought from the parent/carer prior to the uploading of any images.

The use of social networking and media sites

Staff

- Staff are advised not to communicate with or add as 'friends' any current or past students (within three years of leaving) via social media or current or past students' family members via any social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Co-Headteacher or E-safety officer.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (such as email addresses, google apps/ classroom and school telephone).
- Staff are advised to carefully consider the information, including text and images they share and post online and ensure that their use of social media is compatible with their professional role and in accordance with school policies (such as Safeguarding, Confidentiality, Data Protection , Appropriate Conduct).
- Members of staff are encouraged to not identify themselves as employees of the school on their personal social networking sites. This is to prevent information on these sites from being linked with the school and also safeguard the privacy of members of staff and the wider school community.
- Staff are advised to notify the E safety Officer or the Co-Headteacher immediately if they consider that any content shared or posted via any information and communications technology , including emails and social networking sites conflicts with their role in school?

Students

- Students are advised of age restrictions on social media sites, their potential risks and dangers, the need to be respectful of themselves and others at all times online.
- Students are advised to seek the support of an adult and report abusive online behaviours.
- Students are advised to consider the implications of a positive digital footprint for future job employment and or education purposes.

- Staff and students are advised to not use their School email accounts to set up personal online accounts.
- Staff, students and parents/carers are expected not to use social media in such a way to cause grievance to the school or other parents and children.

- Students, staff and parents/carers can seek support via our esafety webpage: http://www.nsg.northants.sch.uk/esafety/ and are invited to interact with the page by recommending useful links and videos

Video-conferencing and web cams
The use of webcams to video-conference with other students or adults is not a facility we currently offer our students. If staff wish to use this form of communication they should inform the e -safety officer and follow the safeguarding guidelines below.

- Students need to ask for permission from a member of staff or adult to use this facility
- Students need to tell an adult immediately of any inappropriate use by another child or adult.
- All students must have written parental consent to participate (more than just a photograph agreement)
- Only school issued equipment should be used
- Ensure that the video conference is supervised at all times by a member of staff
- Have procedures in place for dealing with an unpleasant/unexpected incident during the conference
- Ensuring that the activity is taking place on a secure connection- i.e. cannot be viewed by the public
- Staff manage the storage of the video archive- will a copy of the conference be stored? If so, how long for and who will be able to access it?

E-Safety Support & Advice
Links or feeds to E-Safety websites are provided on our website and new useful guides and links are posted on our front page to support our staff, students and parents in keeping safe online at home / via 3G/4G. The CEOP Report Abuse button is also available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for students to report an incident if they feel they cannot talk to a known adult. CEOP (Child Exploitation and On-line Protection Centre) a link to their website www.thinkukknow.co.uk. The E safety officer is CEOP trained at Ambassador level and leads assemblies and parent session on e safety throughout the year or by request of heads of year or parents.

The E-Safety Code of Practice for staff and the E-Safety Policy will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff in the staff handbook. A copy of the E-Safety Code of Practice for students will be displayed in ICT rooms to remind students of their need to safeguard themselves and others against potential harm from the internet. Records of the students and staff signed codes of practice will be held on file.

Visitors use of personal devices and mobile phones

- Parents carers and visitors must use mobile phones and personal devices in accordance with school policies
- Staff will be expected to challenge concerns when safe and appropriate and will inform the SLT of any breaches by visitors
- Visitors if requiring access to our wifi for professional reasons will be allocated the ‘guest’ wifi login which is protected via a firewall against access to our IT systems and data.

Further Information and Guidance
Please visit the E safety page via the ‘Student’ drop down menu on the school website
http://www.nsg.northants.sch.uk/esafety/

E-Safety Code of Practice for students (Acceptable Use Rules)
I agree that I will:

- never give my password or username to anyone, even my best friend.
- never interfere with others' folders, work or files.
- always report immediately any problem with, or damage to, computer equipment.
- only use the Internet when supervised by a teacher or other adult supervisor agreed by the school
- never give anyone I meet on the Internet personal information about myself or anyone else e.g: my home address, or telephone number or any other private details
- Not disclose my school's name (unless the teacher has given me special permission for a particular purpose)
- never send anyone my picture without permission from my teacher and parent/guardian
- never arrange to meet anyone in person that I have only met online.
- always and immediately tell a member of staff if I see bad language or undesirable/offensive material
- never look for undesirable materials on the Internet
- always show respect for others and never use bad language or write or send words, pictures or videos that could upset or offend others while I am using school computers or the Internet
- never open emails (especially emails with an attachment), download screensavers etc. unless I know who has sent them in case they contain a computer virus.
- never respond to nasty or rude emails or postings in Usenet groups and always report it to a member of staff.
- leave an Internet Chatroom or a Usenet conference at once if someone says/writes something which makes me feel uncomfortable or worried and always report this to a member of staff
- always respect myself and never pretend to be anyone or anything I am not and take the time to consider whether what I am doing is appropriate and safe.
- remember that other people may not be who they say they are.
- remember that information on the Internet may not always be reliable. I will try to evaluate the usefulness and reliability of the information, e.g. by checking other sources or asking my teacher
- Not to use social media in such a way to cause grievance to the school or other parents and children.

I know my teachers and the Internet service provider will check the sites I have visited. I understand **I will not be able to use the Internet if**:

- I deliberately look at unsuitable materials:
- I do not report to a member of staff unsuitable material I discovered accidentally
- I use bad language or deliberately access/send offensive, violent or pornographic material whilst I am online or at any other time when I am using the school's computers
- I use any ICT equipment to produce or send anything which is abusive or hurtful to another person
- I do not follow the guidance on how to prevent computer viruses affecting the school network.
- I access any site by using a proxy site/service.

If there is inappropriate use of the internet:
If there is inappropriate use of the Internet e.g. students get access to undesirable materials, or send offensive messages, teachers will:

- switch off the monitor
- confiscate any printed material or disks
- ensure the school's E safety Policy is followed, i.e. inform the network manager at once
- inform the subject leader for ICT
- write to parents/guardians (sample letter attached)
- The incident in question should be reported to the member of the Senior Leadership Team in charge with the student's name, date, time and room number.
- The network manager/ICT technician staff will immediately deny the student further access to the Internet and will check the student's file for undesirable material and will inform the NSG Technical team so that it can be added to the banned or restricted list
- The student's access to the internet will be removed immediately with a letter sent home.
- Parents will be asked to sign a new ICT Internet Access Policy agreement.
- The new agreement will be discussed with the student/s and parents where appropriate before the access is reinstated.

- If the abuse continues, the school have the right to permanently remove a student's access to the internet.
- The Co-Headteacher will inform the Police or Child Protection Online (CEOP) as necessary.
- I will not store school data on my personal devices, including the downloads folder.

.....

Parents/Guardian's Name:..... Student's Name:.....

- I have read Northampton School for Girls E-Safety Policy and ICT and Internet Access Code of Practice for Students.
- I agree to follow the school's policy and student Code of Practice.

Signed:..... (Student) Date: .....

- I have read the Northampton School for Girls E-Safety Policy and ICT and Internet Access Code of Practice and agree to support the school's policy on the use of ICT and Access to the Internet.
- I have read and discussed the Code of Practice with my child and confirm that she has understood what the code means.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, email and online tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to the policy.
- I understand that whilst my child is using the Internet and other online tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.
- I agree to allow my daughter to use the Internet, electronic mail (email), Google Suite applications, at school.

Signed:..... (Parent/Carer) Date: .....

Appendix I

NSG E – SAFETY CODE OF PRACTICE FOR STAFF

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or email, we are asked to sign this Code of Practice. This is so that we provide an example to students for the safe and responsible use of online technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Personal responsibilities

- I will report any incidents of concern for children's or young people's safety or accidental misuse to the Co-Co-Headteacher & Designated Person for Child Protection (Abigail Boddy) or E-Safety Leader (Paul Parker), in accordance with procedures listed in the E-Safety Policy.
- I know that images should not be inappropriate and should not reveal any personal information about children and young people.

For my protection as an adult working with young people

- I know that if I am using school ICT equipment, including my school laptop to carry out my professional school related duties that it is not advisable to store any personal details / files / photos etc on this school equipment.
- If I am using my own laptop for school duties I will ensure that it is securely protected by antivirus and passwords and that it does not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies. Users may consider encrypting the hard drive to protect personal data.
- I am aware that all electronic devices that are brought into school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items.
- I will check with the ICT technical team before installing any hardware or software onto school equipment and ensure that appropriate licences are in place.
- I will only use my school email address to contact a student via their school email address or to gain any information about a student via the parent or an external agency. *
- I will only use a personal mobile for emergency contact with parents or students and will inform the Co-Headteacher or SLT that I have done so.
- I will not store students mobile numbers on my personal mobile and I am aware that this applies to numbers of students who have left the school in the last three years. If I hold these numbers in my phone I will inform the Co-Headteacher which numbers I hold.
- I will not communicate with current students via social media. For example facebook, adding them as friends. I know that it is recommended practice that this also includes students who have been at the school in the last three years.
- I realise that if I am concerned about the security of a device then I can seek the support from the NSG ICT technical team.
- I will carefully consider the information, including text and images I share and post online and ensure that my use of social media is compatible with my professional role, in accordance with school policies (such as safeguarding, confidentiality, data protection , appropriate conduct)
- I will notify the E safety Officer or the Co-Headteacher immediately if I consider that any content shared or posted via any information and communications technology , including emails and social networking sites conflicts with my role in school
- I will not use my School email accounts to set up personal online accounts.

Security

- I know that I should complete or seek support to complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I keep my passwords secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password or I suspect that someone has used my password I will report it immediately to the E-Safety Leader (PPR).

- I understand that the necessary password length is a minimum of 8 characters and should include numbers as well as letters.
- I will generate a separate password for my SIMS access as it holds very sensitive data.
- I will ensure the data protection of school files by saving to my school Google Drive account, the school servers, or an encrypted portable hard drive or usb stick. *

Knowledge based

- I have a copy of the E-Safety Policy to refer to and I am aware of E-Safety issues and procedures that I should follow.
- I have read and understood my responsibilities as outlined in the associated policies such as; child protection, appropriate conduct with students, behaviour and anti-bullying policies.
- I know that there is training available on e safety as part of the staff training programme should I need to update my knowledge.

Student related professional duties

- I understand that I need to give permission to children and young people before they can use ICT equipment, smartphones etc., to capture images or upload images (video or photographs) to the Internet or send them via email.
- I will adhere to copyright and intellectual property rights and I am aware of my responsibilities regarding data protection (GDPR). *

I have read, understood and agree with this Code of Practice. I know that by following them I am safeguarded from allegations and I understand my responsibilities to safeguard students when using online technologies. I realise that these rules apply to all on-line use and to anything that may be downloaded or printed.

Signed ……. Date: ….....… /……..... / 2019

Name (printed)……

Please note added content marked with * due to GDPR compliance guidelines.
Please return to Sally Tattersfield.

Appendix II

Disciplinary Procedure for All School Based Staff (See also disciplinary procedures policy)

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

School Procedures Following Misuse by Staff

The Co-Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult employed by or working in the school:

A. **An inappropriate website is accessed inadvertently:**
- Report website to the E-Safety Leader (PPR) and the network manager.
- The ICT Technician staff update the filtering service locally so it can be added to the banned or restricted list.

B. **An adult receives inappropriate material:**
- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Co-Headteacher immediately.
- Ensure the device is removed and log the nature of the material. Contact the relevant authorities for further advice e.g. police.
- Inform ICT technicians as in A.

C **An inappropriate website is accessed deliberately. The person discovering this must:**
- Ensure that no one else can access the material.
- Log the incident on a communication form and tick ' E -safety incident'
- Report to the Co-Headteacher and E-Safety Leader immediately.
- Co-Headteacher to refer back to the E safety Policy and the E-Safety Staff code of practice and follow agreed actions for discipline.
- Inform ICT technical team to update the filtering service.

N.B. There are three incidences when we must report directly to the police.

Indecent images of children found.

Incidents of 'grooming' behaviour.

The sending of obscene materials to a child.

It is essential that in such instances that a member of the SLT is informed.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

D. An adult has used ICT equipment inappropriately: Follow the procedures for C.

E. An adult has communicated with a student inappropriately or used ICT equipment inappropriately. The person discovering this must:

- Ensure the student is reassured and remove them from the situation immediately, if necessary.

- Report to the Co-Headteacher and Designated Person for Child Protection (ABY) immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, Local Safeguarding Children Board Northampton (LSCBN).
- Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the E-Safety Policy and E safety Staff code of practice and Co-Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Co-Headteacher or Chair of Governors (if allegation is made against the Co-Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy. Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or any other website or learning platform (or printed out) about a student or an adult in school:

- Preserve any evidence.
- Inform the Co-Headteacher immediately and follow Safeguarding Child Protection Policy as necessary.
- Inform the LA/Local Safeguarding Children Board Northampton (LSCBN) and E-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Co-Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Co-Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a student:

A. An inappropriate website is accessed inadvertently:
Reassure the student that they are not to blame and praise for being safe and responsible by telling an adult. Report website to the E-Safety Leader (PPR) and the network manager. The ICT Technician staff contact the update the filtering service locally so it can be added to the banned or restricted list.

B. An inappropriate website is accessed deliberately:
Refer the student to the Acceptable Use Rules that were agreed. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer.

C. An adult or student has communicated with a student or used ICT equipment inappropriately:
Ensure the student is reassured and remove them from the situation immediately. Report to the Co-Headteacher and Designated Person for Child Protection immediately. Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent. If illegal or inappropriate misuse the Co-Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN. Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a student in school:
Preserve any evidence. Inform the Co-Headteacher immediately. Inform the RBC/LA/LSCBN and E-Safety Leader so that new risks can be identified. Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about a student in the school:
Preserve any evidence. Inform the Co-Headteacher immediately. Follow Acceptable Use Procedures and Anti-bullying policies ensuring that all parents/carers of any students involved are informed of the incident and action taken.

NORTHAMPTON SCHOOL FOR GIRLS

Respect for Self | Respect for Others | Respect for Learning

ONLINE SAFETY

For students and their families

Before You Post

THINK

T - is it True?

H - is it Helpful?

I - is it Inspiring?

N - is it Necessary?

K - is it Kind?

Safety on Social Media?

Young people sometimes share inappropriate or indecent images of themselves online on social media – commonly known as “sexting”, “cybersex” or “sending a nudie”. They may have been coerced or tempted into sending these pictures or videos, perhaps to a friend’s mobile, on a web cam, or on social media. These images are often sent onto others and can end up being used to bully or blackmail the young person.

Young people also use social media for abuse, cyberbullying and intimidation.

Cyber Safety

BE AWARE:

- Sending videos or pictures of yourself to people you don’t know is dangerous
- Sometimes abusers will pretend to be your age.
- Those wanting to take advantage of you will flirt with you; flatter you; make you feel really special
- It can happen to you, to your friend. To boys and to girls.
- Although it may be very common, it can be illegal.

When things go wrong online, many young people are afraid, embarrassed or ashamed to tell someone.

Minimum age: 13

What can you set? Protect your tweets so that only approved followers filter.

What is Twitter?

Twitter, and 'tweeting', is about broadcasting daily short burst messages to the world, with the hope that your messages are useful and interesting to someone. In other words, *microblogging*.

Twitter is a blend of instant messaging, blogging, and texting, but with brief content and a very broad audience. People send Twitter 'tweets' for all sorts of reasons: vanity, attention, self-promotion of their web pages, boredom. The great majority of tweeters do this microblogging as a recreational thing, a chance to shout out to the world and revel in how many people choose to read your stuff.

can see them, hide certain users tweets from your timeline, block people from contacting you and make use of the quality

BE AWARE: Whatever you 'Tweet' - it's PUBLIC!

Minimum age: 13

What is Instagram?

Instagram is an online mobile photo-sharing site that enables its users to take pictures and share them either publicly or privately on the app, as well as through a variety of other social networking platforms. When you post a photo or video on Instagram, it will be displayed on your profile. Other users who follow you will see your posts in their own feed. Likewise, you'll see posts from other users who you choose. Just like other social networks, you can interact with other users on Instagram by following them, being followed by them, commenting, liking, tagging and private messaging or follow.

You can sign up via your existing Facebook account or by email. When you start following people and looking for people to follow you back, they'll want to know who you are and what you're all about.

BE AWARE: It's public!

snapchat

Minimum age: 13

What is Snapchat?

Snapchat is a mobile app that allows you to send videos and pictures, both of which will self-destruct after a few seconds of a person viewing them.

Snapchat is also a messaging app. You can capture a photo or brief video with it, then add a caption or doodle or filter/lens over top, and send the finished creation (called a snap) to a friend. Alternatively, you can add your snap to your "story", a 24-hour collection of all your snaps that's broadcasted to the world or just your friends, or followers.

Your friends can view snaps for up to 10 seconds, and then the snaps disappear. You can also save your own snaps before sending them to friends or you story. You can reply to spans. You can use Snapchat to chat and video chat. On a screen you can have conversation with your friend.

BE AWARE: A screenshot can be taken of your sent snap picture or chat and shared to public! Your videos also can be uploaded to a compute!

YouTube

Minimum age: 13

What can you set: watch, create, share videos, create channels, write comment, personalize and block.

What is YouTube?

YouTube is a free video sharing website that makes it easy to watch online videos. You can even create and upload your own videos to share with others.

Once uploaded, other YouTube users can leave rate or leave comments about the video, as well as post a YouTube video response. Videos transferred to YouTube are converted to Adobe Flash files so all users can view the videos without having to worry about getting extra software or plug-ins.

BE AWARE: YouTube can be risky due to advertising, inappropriate content, bullying or rude comments.

Minimum age: 12+

What is TikTok?

TikTok is a video-sharing social media app which lets users create, share, and view user created videos much in a similar manner to Facebook, Instagram and snapchat. Its main draw is that users can record and upload bite-sized looping videos of themselves lip-syncing and dancing to popular music or soundbites, often for comedic effect, which can then be further enhanced with filters, emojis and stickers. TikTok has been designed with the young user in mind and has a very addictive appeal. At the beginning of 2019 it skyrocketed in popularity to become the most downloaded app.

BE AWARE: that by default, any user can comment on your child's video if their account is set to public.

Minimum age: 13

What can you set? Decide who sees your posts and Timelines, unfriend people and block.

What is Facebook?

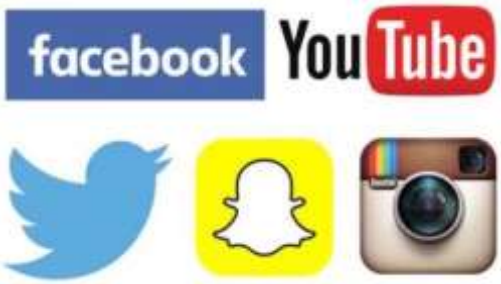
Facebook is a social networking website and service where users can post comments, share photographs and links to news or other content on the Web, play games, chat live, and even stream live video. Shared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with a single person. Facebook allows you to maintain a friends list and choose privacy settings to tailor who can see content on your profile. Facebook allows you to upload photos and maintain photo albums that can be shared with your friends. Facebook supports interactive online chat and the ability to comment on your friend's profile pages, called "walls," in order to keep in touch.

BE AWARE: Facebook is public and even if you post something and delete it, doesn't mean that someone didn't take a screenshot of it before you had the chance to

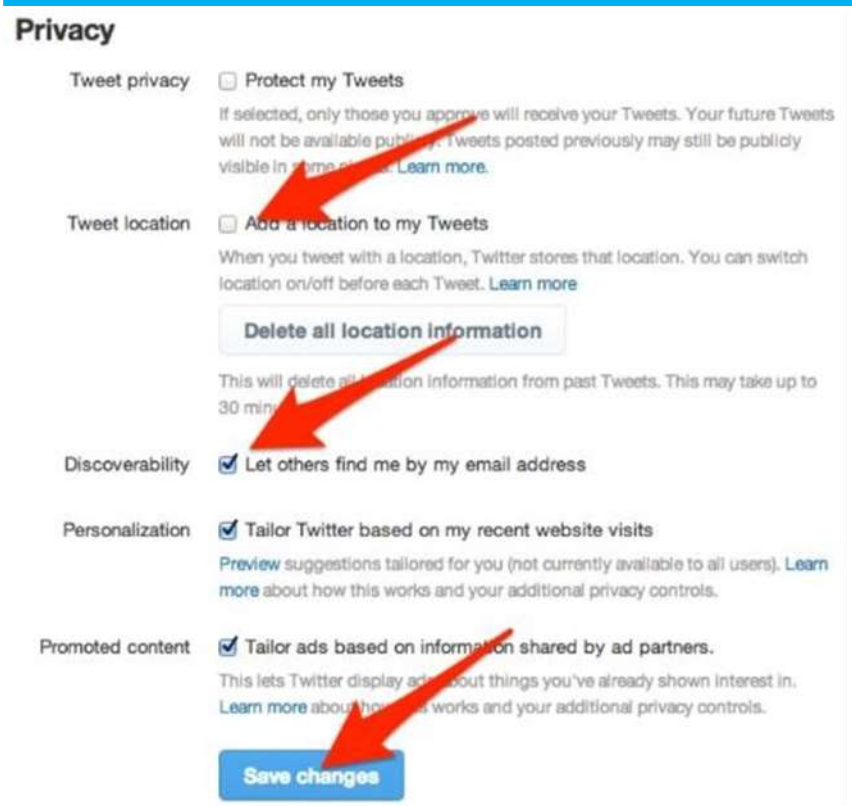

safebook
YOU
THINK
Think before you post
FRIENDS
Only connect with friends
KIND
Be kind to others
PASSWORD
Don't share your password
PRIVACY
Keep your settings private
HURT
Don't be hurtful towards others
PARENTS & TEACHERS
Join Facebook
Understand how it works
Teach safety and responsibility
Privacy – check their settings
FRIENDS
DON'T: Stay silent
DO: Help your friend
Report the bully
Tell your parents
Tell your teacher
THE BULLY
DON'T: Respond
DO: Save what they say
Unfriend the person
Block them
Tell a Friend
Tell your Parents
Report the person
TELL • UNFRIEND • BLOCK • REPORT

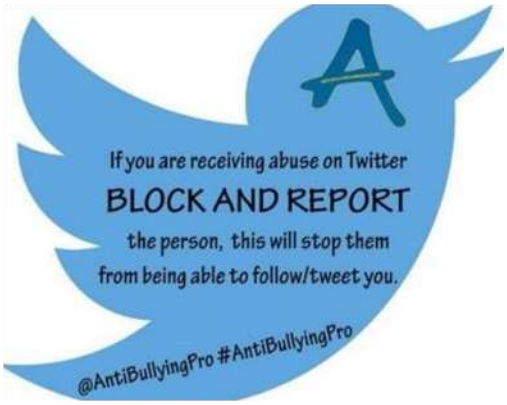

Keeping Safe Online
Nicknames
It is a good idea to use a nickname or a screenname instead of your real name.
Passwords
Never use personal information such as your name or birthday.
Be Scam Smart
Never open strange emails, beware of free downloads and don't use peer-to-peer file sharing it can leave you open to viruses.
01
02
03
04
05
Report bad content
Report bad content immediately. If you come across bad comments or pictures talk to your parents or teachers.
Personal Info
Don't give out personal information such as addresses, phone numbers, passwords and pictures.

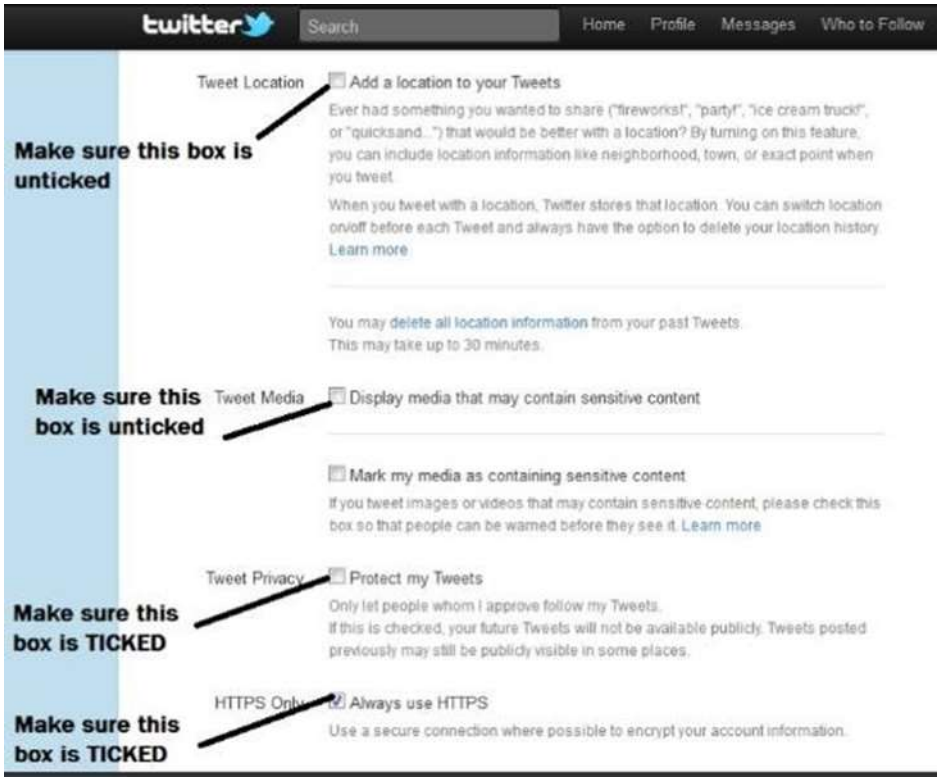
Protecting your Privacy on social media



How to set privacy settings


Privacy
Tweet privacy
Protect my Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.
Tweet location
Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more
Delete all location information
This will delete all location information from past Tweets. This may take up to 30 min
Discoverability
Let others find me by my email address
Personalization
Tailor Twitter based on my recent website visits
Preview suggestions tailored for you (not currently available to all users). Learn more about how this works and your additional privacy controls.
Promoted content
Tailor ads based on information shared by ad partners.
This lets Twitter display ads about things you've already shown interest in.
Learn more about how this works and your additional privacy controls.
Save changes


If you are receiving abuse on Twitter
BLOCK AND REPORT
the person, this will stop them
from being able to follow/tweet you.
@AntiBullyingPro #AntiBullyingPro


twitter
Search
Home
Profile
Messages
Who to Follow
Tweet Location
Add a location to your Tweets
Ever had something you wanted to share ("fireworks!", "party!", "ice cream truck!", or "quicksand...") that would be better with a location? By turning on this feature, you can include location information like neighborhood, town, or exact point when you tweet.
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet and always have the option to delete your location history. Learn more
You may delete all location information from your past Tweets.
This may take up to 30 minutes.
Make sure this box is unticked
Tweet Media
Display media that may contain sensitive content
Mark my media as containing sensitive content
If you tweet images or videos that may contain sensitive content, please check this box so that people can be warned before they see it. Learn more
Make sure this box is unticked
Tweet Privacy
Protect my Tweets
Only let people whom I approve follow my Tweets.
If this is checked, your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.
Make sure this box is TICKED
HTTPS Only
Always use HTTPS
Use a secure connection where possible to encrypt your account information.
Make sure this box is TICKED

Instagram

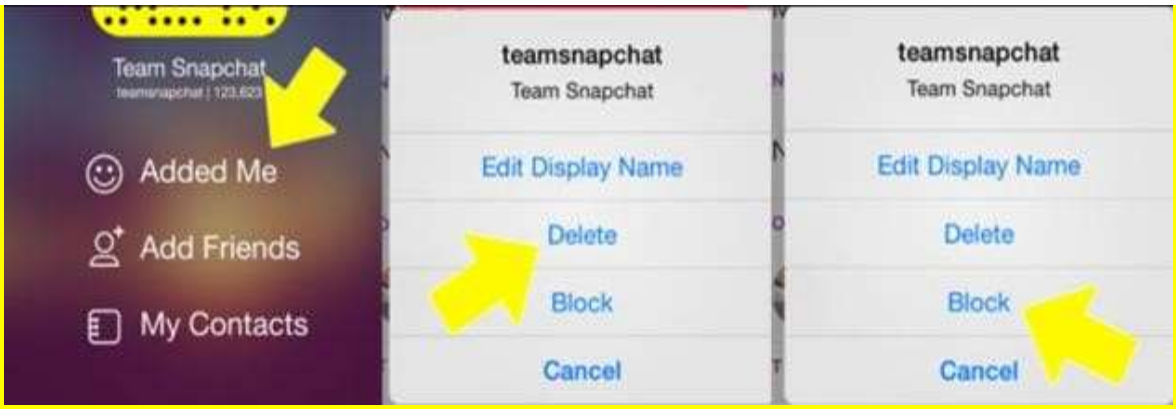

LEONIEGSMITH
728
59
69
Edit Your Profile
Leonie Smith
Cyber Safety Cat Lady. Jazz Diva .
www.thecybersafetylady.com.au
thecybersafetylady.com.au
1
2

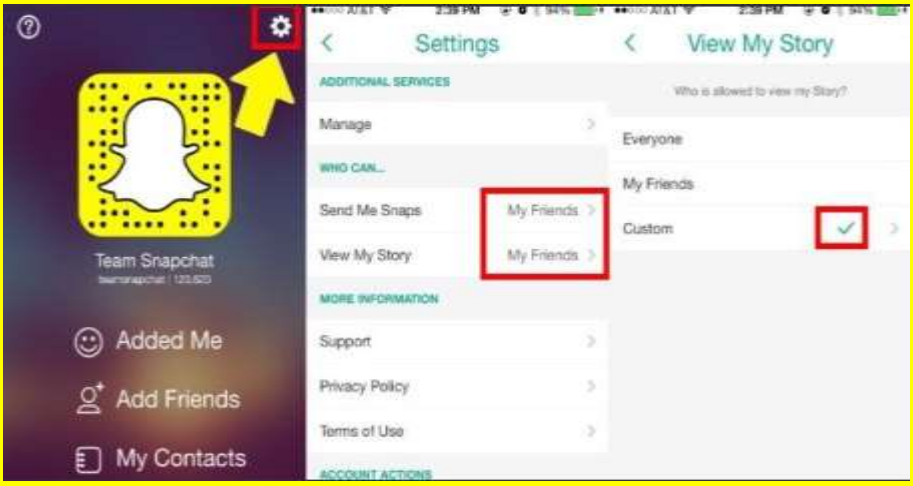

OPTIONS
FOLLOW PEOPLE
Find Facebook Friends
Find Contacts
Invite Friends
ACCOUNT
Edit Profile
Change Password
Posts You've Liked
Private Account
3


Instagram Stories
Privacy Options
Verizon
7:19 PM
84%
Instagram
Your Story
Verizon
2:11 PM
79%
Story Settings
Hide Story From
2 People
ALLOW MESSAGE REPLIES
Your Followers
Followers You Follow Back
Off
Choose who can reply to your story.

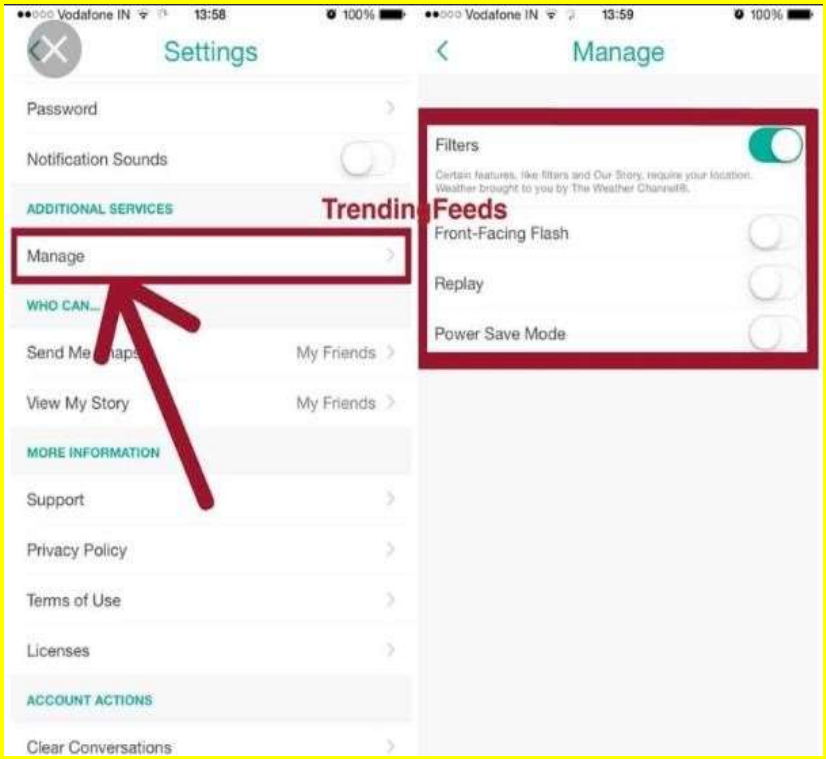

Share to
FOLLOWERS
DIRECT
Write a caption...
Tag People
Add to Photo Map
Facebook
Twitter

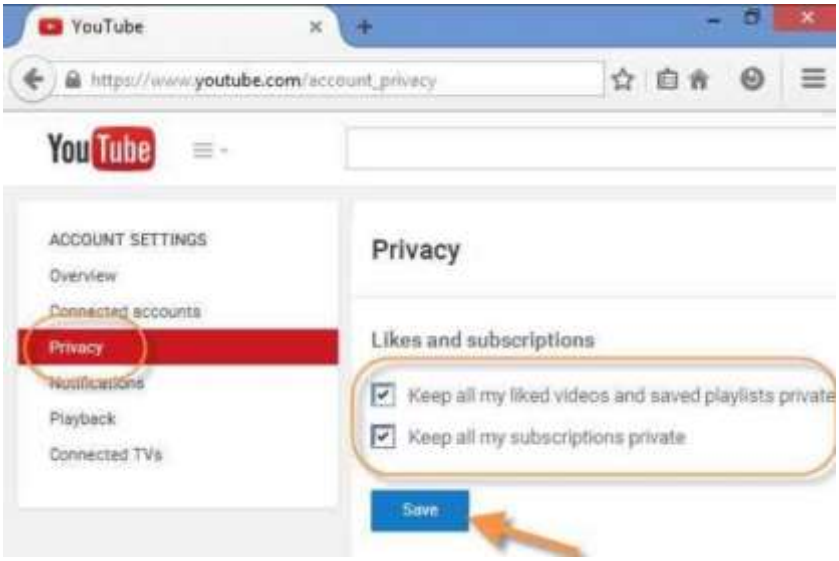
snapchat



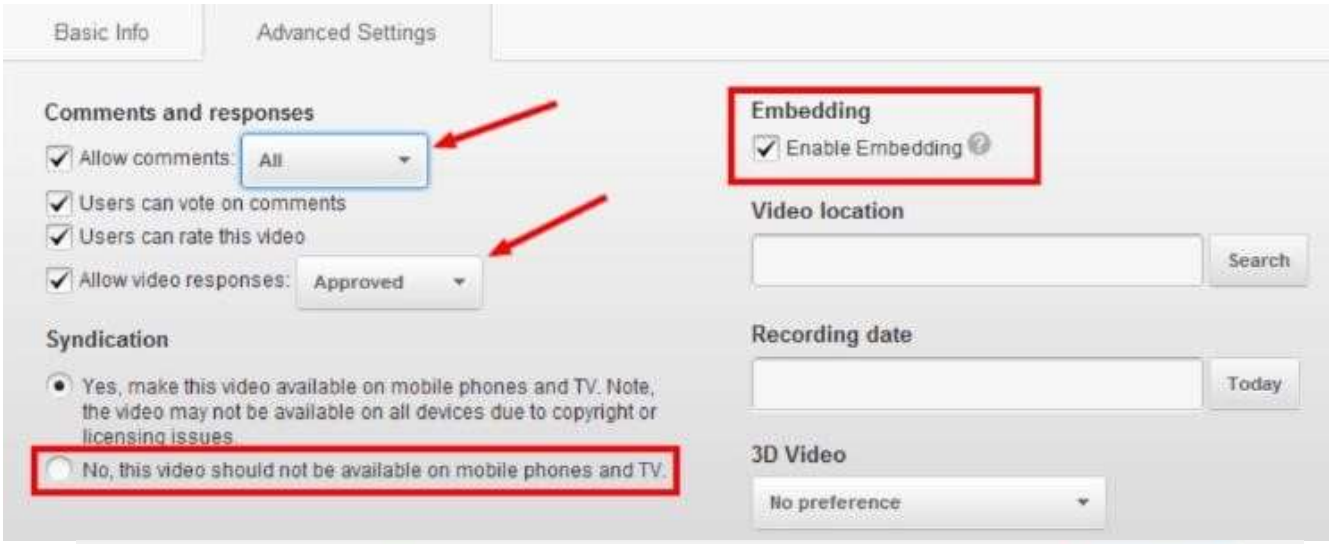


Snapchat:offers users the ability to send and receive messages, photos, or videos that disappear after few seconds.**Problem:**It is the #1 app used for sexting. Many of the files uploaded to Snapchat end up on revenge porn site, called 'snap porn'.




YouTube
https://www.youtube.com/account_privacy
YouTube
ACCOUNT SETTINGS
Overview
Connected accounts
Privacy
Notifications
Playback
Connected TVs
Privacy
Likes and subscriptions
Keep all my liked videos and saved playlists private
Keep all my subscriptions private
Save


YouTube
Change YouTube
Privacy Settings


Basic Info
Advanced Settings
Comments and responses
Allow comments:
All
Users can vote on comments
Users can rate this video
Allow video responses:
Approved
Syndication
Yes, make this video available on mobile phones and TV. Note, the video may not be available on all devices due to copyright or licensing issues
No, this video should not be available on mobile phones and TV.
Embedding
Enable Embedding
Video location
Search
Recording date
Today
3D Video
No preference


UPLOADING 13%
6 minutes remaining.
Publish
Your video is still uploading. Please keep this page open until it's done.
Basic info
Advanced settings
FUNNY VIDEOS Funny Cats Funny Cat Videos Funny Animals Fail C
Public
Description
Add a message to your video
Also share on
Suggested tags
+ Cat (Animal)
+ Funny
+ Comedy
+ Clips
+ Cats
VIDEO THUMBNAILS

TikTok

1

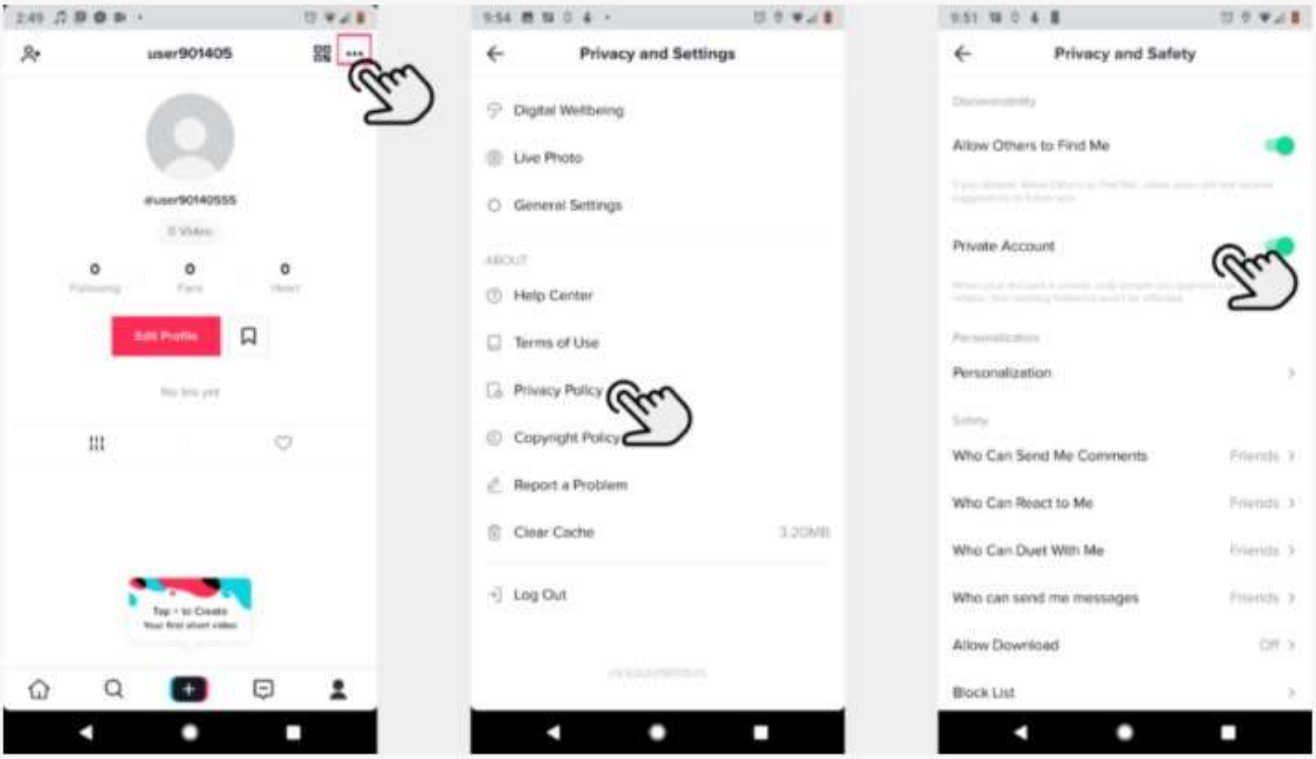
How to make TikTok account to private

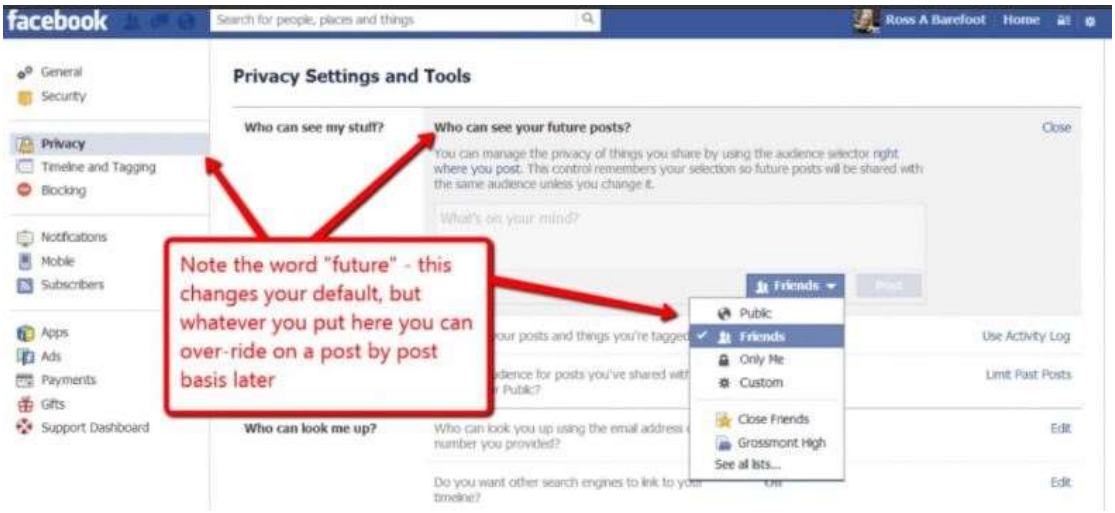
Please note that even with a private account your child's profile photo, username, and bio will be visible to all TikTok users. It is best to ensure no sensitive or personal information is included here.

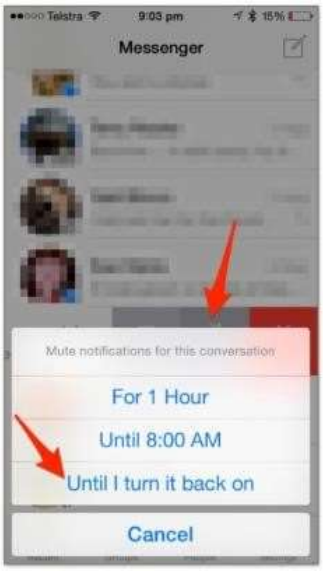
Step 1- Go to your profile page

Step 2– Tap three dots on the top right corner and select "Privacy and Settings"

Step 3 – Select "Privacy and Safety" option and toggle "Private Account" on/off







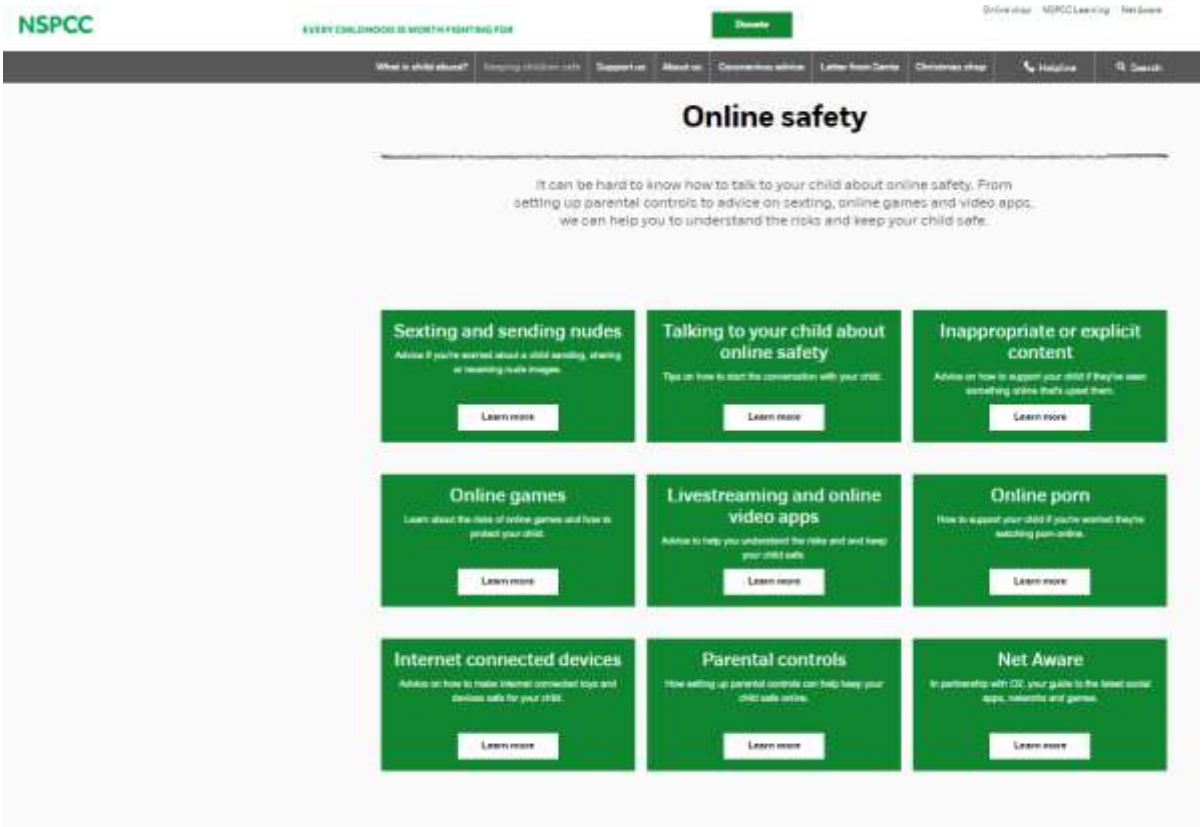
Swipe left, select "Mute" Option and select 'Until I turn it back on"

Swipe left, select "More" Option and select "Mark as Spam"

To Block, click on message click the (i) icon. Click "More" and "Block"

Additional Information for Parents and Carers

NSPCC website https://www.nspcc.org.uk/keeping-children-safe/online-safety/ offers parents support with specific issues



Also linked to the NSPCC site is this family agreement resource and ideas about how to create a family agreement with older children

Alternatively, Childnet International suggest the following

There are real advantages in maintaining an open dialogue with your child about their internet use.
Not sure where to begin? These conversation starter suggestions can help.

1. Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
2. Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
3. Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
4. Encourage them to help someone! Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
5. Think about how you each use the internet. What more could you do to use the internet together? Are there activities that you could enjoy as a family?

What can I do right now?

- ☐ Maintain an open dialogue with your child and encourage them to talk to you about their internet use: for example who they're talking to, services they're using, and any issues they may be experiencing.
- ☐ Create a family agreement to establish your children's boundaries, and your expectations, when on the internet. A template agreement can be found at www.childnet.com/have-a-conversation
- ☐ Give your child strategies to deal with any online content that they are not comfortable with – such as turning off the screen, telling an adult they trust and using online reporting facilities.
- ☐ Consider using filtering software to block unwanted content. In addition to filtering, remember that discussion with your child, and involvement in their internet use, are both effective ways to educate them about the internet.
- ☐ Encourage your child to 'think before you post.' Online actions can impact not only yourself but the lives of others. Content posted privately online can be publicly shared by others, and may remain online forever.
- ☐ Understand the law. Some online behaviour may break the law, for example when downloading or sharing content with others. Be able to recommend legal services.
- ☐ Familiarise yourself with the privacy settings and reporting features available on popular sites, services and apps.
- ☐ If your child is being bullied online, save all available evidence and know where to report the incident, for example to the school, service provider, or the police if the law has been broken.
- ☐ Familiarise yourself with the age ratings for games and apps which can help to indicate the level and suitability of the content. Also see if online reviews are available from other parents as these may be helpful.
- ☐ Set up a family email address that your children can use when signing up to new games and websites online.
- ☐ Encourage your child to use nicknames (where possible) instead of their full name online, to protect their personal information, and create strong passwords for every account.

Sign up to our Childnet newsletter at www.childnet.com.

6 Tips for Teens:

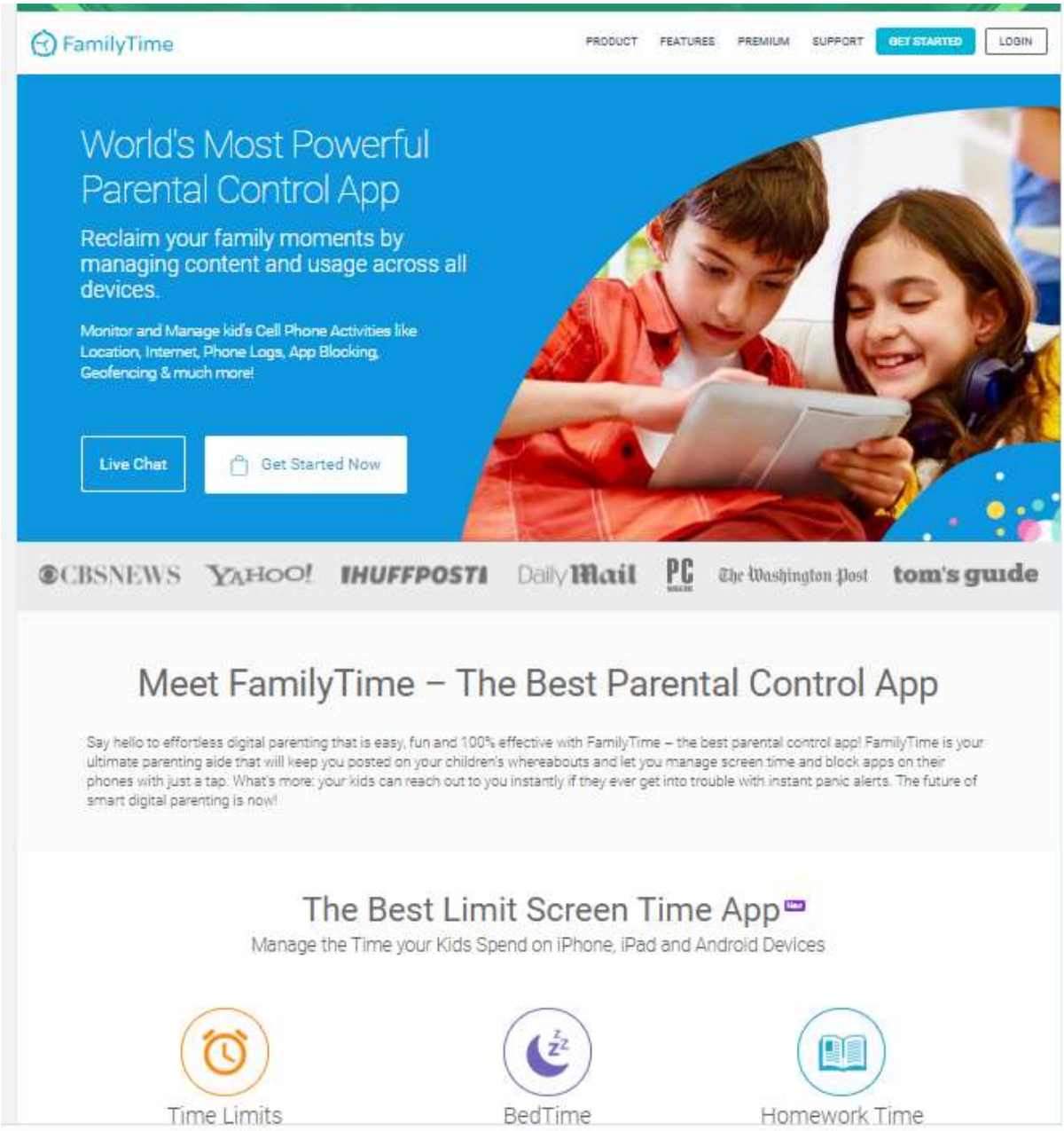
1. **Protect your online reputation:** use the tools provided by online services to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.
2. **Know where to find help:** understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone.
3. **Don't give in to pressure:** if you lose your inhibitions you've lost control; once you've pressed send you can't take it back.
4. **Respect the law:** use reliable services and know how to legally access the music, film and TV you want.
5. **Acknowledge your sources:** use trustworthy content and remember to give credit when using other people's work/ ideas.
6. **Be a critical thinker:** not everything or everyone is trustworthy; think carefully about what you see and experience on sites, social media and apps.

Further advice and resources:

www.childnet.com

www.saferinternet.org.uk

Family time is a subscription service that can support parents to monitor and control their child's access to social media https://familytime.io/get-started.html



Remember you can get support from

CEOP: https://www.thinkuknow.co.uk/

Childline: https://www.childline.org.uk/

Northampton Local Authority: http://www.northamptonshirescb.org.uk/parents-carers/esafety/

Or contact your child's head of year at school.

Telephone number: 01604 679540

Email: admin@nsg.northants.sch.uk