# Session 6 - Technology and the internet at home

|  |  |
| --- | --- |
| **Resources** | |
| Resource Sheet 1 – Family Apps | A copy for each student or pair of students |
| Resource Sheet 2 – Family Apps Answers | A copy for each student or pair of students |
| Activity 1 – online risks | Sticky notes  4 flip chart sheets or whiteboard with headings  1.Interference from others  2.Tracking of my internet use and use of data by website/social media and their partners  3.Inappropriate content,  4.Influencing, controlling, intimidating or abusive communication |
| Resource Sheet 3 – Risks and settings | A copy for each student |
| Resource Sheet 4 – Risks and good online habits | A copy for each student |
| Reporting risks website | Computer, projector and screen |
| My evaluation sheet | Each student has a copy |
| My Acceptable User Policy | Each student has a copy |

**Intended learning outcomes: ‘I …’ statement(s)**

|  |
| --- |
| I accept the need to install security updates  and antivirus software on all of the devices that my family owns, as well as update passwords and codes  I know what I need to do for myself if I have a problem online outside of school  I know what acceptable and healthy use of the internet at home looks like |

**Note: One of the SEL foci of this session is identifying risk. It may emerge that participants may not recognize or fully appreciate the risks of internet use and require support with the Core Activities.**

|  |
| --- |
| **Facilitator tip:** If you are not already combining sessions for parents/carers and students, you may wish to invite parents/carers to join their children for this session so that they work together to think about internet safety in their home. |

**Welcome**

Welcome students and ask whether they have done anything to support a friend online since our last session.

**Warm-up activity: Popular apps/websites/devices**

**Purpose:** To consider students’ online activities and restrictions that apply to children

Give out Resource sheet 1. Ask students to work in pairs to identify each of the 'Family Apps'  on the sheet and to record the age they think a person needs to be to have access to it.

Use the Resource Sheet 2 'Answers' to discuss outcomes and to emphasise the point that, apart from Moshi Monsters (which has no age restriction), **all the apps have an age restriction of 13**. However, YouTube not only requires users to register if they want to post videos; it offers a separate 'YouTube Kids' platform.

|  |
| --- |
| **Facilitator tip**: Alternatively you could cut Resource Sheets 1 and 2 into cards. Pairs of students could play a game of 'What App Am I?' with one participant holding one of the unseen cards from Resource Sheet 1 to their forehead and asking their partner questions in order to guess the app (the partner uses a card from the Resource Sheet 2 'Answers' sheet to respond to the questions). |

**Review group aims:**

Explain that, today, we are going to think about how we use the internet at home. Do the rules we have agreed apply just as much there as they do here?

**Plan for today’s session**

Explain that, today, we will work on these learning outcomes for each student in the group.

* I accept the need to install security updates and antivirus software on all of the devices that my family owns, as well as update passwords and codes
* I know what I need to do for myself if I have a problem online outside school
* I know what acceptable and healthy use of the internet at home looks like

Ensure they understand what the learning outcomes mean and tell them you will be asking them at the end of the session to think about whether they think they have been achieved.

**Core Activity 1: Online risks**

**Purpose:** to begin a conversation about the risks of being online and discover how aware students are of them

Prepare 4 flip chart sheets or whiteboard with headings:

1. Interference from others

2. Tracking of my internet use and use of data by website/social media and their partners

3. Inappropriate content,

4. Influencing, controlling, intimidating or abusive communication

Ask students to work in small groups. Give them some sticky notes and ask them to list all the risks that they can think of regarding their online activity. They should write each risk on a separate sticky note.

Explain that we are going to arrange the risks under 4 headings by putting each sticky note on the appropriate place on a flip chart sheet/whiteboard. Ask for an example of each category (Resource sheet 3 lists relevant examples) to ensure they understand the task.

|  |
| --- |
| **Facilitator tip:** To encourage students to consider each other’s contributions, ask them, when they post their sticky notes, to read the others and, if another group has posted a note with the same idea as them, to place their sticky note of top of it. |

When they have finished, discuss their ideas

**Core Activity 2: Risks and settings**

**Purpos**e: To consider ways of minimising the risks of being online

Give out Resource Sheet 3. Ask students to look at the risks listed in the 1st column. Are there any they want to add from the ones they identified in the last activity?

Explain that the 2nd column provides information about setting up devices to prevent these risks and ask participants to add ticks, crosses or question marks to evaluate whether these actions have been '**Done', 'Not Done'**at home**,**or whether they're **'Not Sure'**

**Core Activity 3: Risks and good online habits**

**Purpose:** to help students to increase their online safety

Give out Resource Sheet 4. Ask students to work in pairs to discuss and complete it individually.

Ask participants to look at their lists on Resource Sheets 3 and 4 and consider how safe they feel their family is when it goes on the internet at home.  Is there anything they want to do to make them safer?

|  |
| --- |
| **Facilitator tip:** The aim in this session is to raise students’ awareness of risks but not to leave them over-anxious about them. We all face these risks and need to know how to minimize them.  They may wish to take Resource sheet 3 home to discuss with their parents/carers.  If you intend to run parallel ICAMcsr session for parents/carers, you can reassure students that you will be discussing these issues with them too. |

**Core Activity 4: Reporting concerns**

**Purpose**: to ensure that students know what to do if they have concerns about their safety oinline

Stress the importance of talking to adults about any concerns students’ have about their internet safety.

Show and discuss the website <https://www.internetmatters.org/report-issue/>  which explains how to report problems

**Review and reflection on intended learning outcomes and group aims**

Ask the students to indicate how well they feel they have achieved the session learning outcomes by using ‘thumbs up, thumbs level or thumbs down’. If students indicate that they haven’t achieved the learning outcome ask why and ensure that you plan the next sessions accordingly, or offer further support if possible.

Ask them to complete their evaluation sheet and personal Acceptable User Policy for Session 6

**Note: Students may experience anxiety regarding their family's online safety and require additional support in undertaking the actions that they have identified in the activities in this session. It may be necessary to be mindful of the school’s safeguarding protocols and follow procedures if issues arise.**

**Session 6. Resource Sheet 1: Family Apps**

Describe what each of these Apps can do and how old you have to be to use it. The first row is completed as an example.

|  |  |  |
| --- | --- | --- |
| **App** | **What Is It?** | **Age Restriction** |
|  | A social networking site where users can ask each other questions | 13 |
|  |  |  |
| A picture containing person, player, racket, holding  Description automatically generated |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Session 6. Resource Sheet 2: Family Apps- Answers**

|  |  |
| --- | --- |
| **App** | **What Is It?** |
|  | A social networking site where users can ask each other questions |
|  | A popular social network with over a billion users.  where uses create profiles and share views/experiences and images |
| A picture containing person, player, racket, holding  Description automatically generated | A survival action game where up to 100 live players can fight each other to be the last one standing; it includes heavy violence but with little blood or gore. You can talk to other players using public, private and voice chat. |
|  | A photo and video sharing app, popular with teens: connection with one another is made through comments, captions and hashtags on photos and videos. |
|  | An online social game popular with 6-12 year olds that allows children to choose, customise and nurture a pet monster. Children can play games, solve puzzles and explore ‘Monstro City’ with their pet. |
|  | A messaging app that is popular with teenagers, for sharing photos, texts and videos, ie ‘snaps’ for only 10 seconds before disappearing. ‘Snapstory’ allows users to share ‘snaps’ with others for 24 hours. |
|  | A social media platform for users to share short videos of themselves performing songs, dances, lip synchs, comedy etc |
|  | A social networking and microblogging site where users post 'tweets' that are 140 characters long and can include images or videos. |
|  | A video-sharing website |

**Session 6 . Resource Sheet 3 : Risks and settings**

|  |  |  |
| --- | --- | --- |
| **Risks** | **Settings and Assistance on Devices** | * **= Done**   **X = Not Done**  **? = Not Sure** |
| **Interference from others**  *e.g hacking*  *viruses*  *phishing (illegal attempts to gain personal information)*  *ransomware (software that secures personal data or blocks access to it which can only be reversed, following payment of a ‘ransom’)* | Set up password for home wi-fi router that only the family knows  Ensure your [Wi-F is secured](https://www.getsafeonline.org/protecting-your-computer/wireless-networks-and-hotspots-pyc/) to [WPA2](https://www.getsafeonline.org/protecting-yourself/the-internet-of-things/) level at all times and do not reveal the access code to unauthorised persons.  Set up firewalls  (*Windows: Right Click Windows logo > Control Panel > Security > Firewall*  *Mac OS: Click Apple logo > System Preferences > Privacy & Security > Firewall*  Set parent controls on computers and mobile phones/iPads  Set parent controls on internet service provider - BT, Sky, Virgin Media and TalkTalk provide access to this facility free of charge  Download parent control software that allows monitoring of online activity by others  Create and update different ‘strong’ passwords for different devices (including smart speakers, televisions, child monitors and programmable electrical devices) and different online accounts  Install antivirus/antispyware and keep it up to date  Only allow downloads from identified developers – option available in ‘Security’ settings  Set Parent Controls to ‘Limit Mail to allowed contacts’  Set spam/junk email filters to block emails from untrusted sources – keep the feature updated and switched on  Install software updates, including operating systems and games, when prompted, as they usually contain new security measures  Back-up data on to a remote device  Avoid open wi-fi (such as wi-fi offered in stores, cafes etc…) when providing personal information (unless the website is secure) – a mobile network (such as 4G) is more secure  Don’t allow anyone to connect a device to yours  Be careful with CDs/DVDs as they can also contain viruses. |  |
| **Tracking internet use and use of data by website/social media ‘partners’**  *e.g.Targeted advertisements /post*  *Junk mail / SPAM* | Parent Controls – switch off ‘Allow use of camera’  Switch off functions in Smart Speakers that allow the makers to monitor conversations  Switch on ‘block cookies’ in Privacy section of search engine settings (some websites may not work as a result) |  |
| **Inappropriate content**  *e.g.Violent or sexual images*  *Messages that encourage children/young people to take part in criminal activities* | Switch on search engine/browser warning regarding safety certificates of websites |  |
| **Influencing, controlling, intimidating or abusive communication**  *Cyber-bullying*  *Trolling*  *Attempts to radicalise* | Set Parent Controls to ‘Limit Mail to allowed contacts’ |  |

**Session 6 . Resource Sheet 4 : Risks and good online habits**

|  |  |  |
| --- | --- | --- |
| **Risks** | **Settings and Assistance on Devices** | * **= Done**   **X = Not Done**  **? = Not Sure** |
| **Interference from others**  *e.g. hacking*  *viruses*  *phishing (illegal attempts to gain personal information)*  *ransomware (software that secures personal data or blocks access to it which can only be reversed, following payment of a ‘ransom’)* | Report ransomware or fraud immediately by calling Action Fraud: **0300 123 20 40** or by visiting [www.actionfraud.police.uk](http://www.actionfraud.police.uk)  Only open emails from recognized contacts  Don’t respond to blackmail emails or click on links  Change passwords (and ‘secret questions’) of any accounts that are mentioned in blackmail emails and contact the company  If you use your phone to make payments, treat it like your wallet and makes sure it is always locked with a PIN  Always log out of banking apps  Remember that your bank will never contact you to ask for your account details, passwords or PINs  Only use websites that end in ‘gov.uk’ for official services, such as passports, birth certificates, driving licences – search for them rather than the first ones to appear in your search engine  Check for the number of followers of a social media account that has shared an unusual or unexpected message – the larger the number, the more genuine it could be  Only buy goods (including games) from trustworthy sellers (research them first) with known addresses – check that the payment page is secure and only pay by card  Install apps from trusted sources and check age ratings  Use a disposable anonymous [webmail](https://www.getsafeonline.org/protecting-yourself/privacy/) account for websites that demand an email address to register  Check with friends if you receive unexpected or unusual messages from them |  |
| **Tracking internet use and use of data by website/social media ‘partners’**  *e.g. Targeted advertisements /post*  *Junk mail / SPAM* | Encourage family to manage privacy settings on websites (rather than ‘Accept All’)  Encourage family to only enter private information on websites that have addresses starting with ‘https://’ or when a padlock symbol appears on the browser window (not the web page itself)  Check Terms and Conditions and permissions of apps for details of the amount and nature of the data that they want to access (and use)  Download the information that Facebook holds about you  Think carefully before allowing apps to access your ‘current location’ |  |
| **Inappropriate content**  *e.g. Violent or sexual images*  *Messages that encourage children/young people to take part in criminal activities* | Consider using the ‘UK only’ option from search engines, as UK-hosted sites are subject to UK law  Check sources before downloading (children need to ask permission)  Take care about opening attachments  Check for spelling mistakes or a lack of personal address (your name)  Only open emails from recognized contacts  Report Hate Content to providers (social media platforms, administrators, hosts\*, search engines or internet service providers)  *\*You can check a website’s hosting company by entering their web address on the website*[***‘Who is hosting this website?’***](http://www.satoristudio.net/who-is-hosting)*.*  Check age ratings for games  Check for hidden charges created within games |  |
| **Influencing, controlling, intimidating or abusive communication**  *e.g. Cyber-bullying*  *Trolling*  *Attempts to radicalise* | Keep your personal online (including gaming and social media) information to a minimum  Block people who send unwelcome messages  If necessary, be prepared to change accounts if unwelcome messages persist  Arrange to talk with trusted friends who appear to send you unwelcome messages – their technology or accounts may have been ‘borrowed’ by others    Change passwords regularly  Collect evidence and report it to the police  Report abuse/cyber-bullying to the relevant provider (social media platforms, administrators, hosts\*, search engines or internet service providers)  Report personal approaches to influence your thinking about extremist/terrorist activities to the police in confidence: 0800 789 321  Seek support from family, friends and/or organizations, such as:  Childline 0800 1111  NSPCC 0808 800 5000  National Stalking Helpline **0808 802 0300**  **Avoid replying, unless you feel confident that you can challenge attempts to bully you in an assertive (not aggressive or passive) manner or you can pretend that you don’t know what they’re trying to do (see advice regarding ‘Fogging’)**  **Have children play online games in shared family space, using computer or tv speakers rather than headphones so that the language of players can be monitored** |  |