



Computing

Scheme of Work

Unit 4.2 – Online Safety



Year Group: 4
Number of
Lessons: 4



From **2**simple



Contents

Introduction	3
Year 4 – Medium-term Plan	4
Lesson 1 – Going Phishing	5
Aims.....	5
Success criteria	5
Resources	5
Lesson 2 – Beware Malware	10
Aims.....	10
Success criteria	10
Resources	10
Activities	10
Lesson 3 – Plagiarism	13
Aims.....	13
Success criteria	13
Resources	13
Activities	13
Lesson 4 – Healthy Screen-time	15
Aims.....	15
Success criteria	15
Resources	15
Activities	15
Assessment Guidance	18



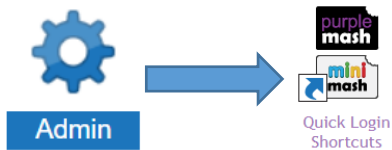
Introduction

For these sessions, the children will need to have their own individual logins to Purple Mash.

If you are currently using a single login per class or group and would like to set up individual logins yourself, then please see our guide to doing so at [Create and Manage Users](#). Alternatively, please contact support at support@2simple.com or 0208 203 1781.

Check with the Purple Mash Administrator in your school (usually the coordinator) if you need to change the children's passwords. You can create picture passwords for the younger children but if you're not sure how to do this just give the 2Simple office a call and we can talk you through it or set them up for you!

Your school administrator can put a shortcut to your school's Purple Mash portal on the devices so there is an icon to use for Purple Mash to save time when the children are logging in. The tool to do this can be found in the Admin tab:





Year 4 – Medium-term Plan

Lesson	Aims	Success Criteria
<u>1</u>	<ul style="list-style-type: none"> To understand how children can protect themselves from online identity theft. Understand that information put online leaves a digital footprint or trail and that this can aid identity theft. 	<ul style="list-style-type: none"> Children know that security symbols such as a padlock protect their identity online. Children know the meaning of the term 'phishing' and are aware of the existence of scam websites. Children can explain what a digital footprint is and how it relates to identity theft. Children can give examples of things that they wouldn't want to be in their digital footprint.
<u>2</u>	<ul style="list-style-type: none"> To Identify the risks and benefits of installing software including apps. 	<ul style="list-style-type: none"> Children can identify possible risks of installing free and paid for software. Children know that malware is software that is specifically designed to disrupt, damage, or gain access to a computer. Children know what a computer virus is.
<u>3</u>	<ul style="list-style-type: none"> To understand that copying the work of others and presenting it as their own is called 'plagiarism' and to consider the consequences of plagiarism. To identify appropriate behaviour when participating or contributing to collaborative online projects for learning. 	<ul style="list-style-type: none"> Children are able to determine whether activities that they undertake online, infringe another's' copyright. They know the difference between researching and using information and copying it Children know about citing sources that they have used.
<u>4</u>	<ul style="list-style-type: none"> To identify the positive and negative influences of technology on health and the environment. To understand the importance of balancing game and screen time with other parts of their lives. 	<ul style="list-style-type: none"> Children are able to take more informed ownership of the way that they choose to use their free time. They recognise a need to find a balance between being active and digital activities. Children can give reasons for limiting screen time.



Lesson 1 – Going Phishing

Aims

- To understand how children can protect themselves from online identity theft.
- Understand that information put online leaves a digital footprint or trail and that this can aid identity theft.

Success criteria

- Children know that security symbols such as a padlock protect their identity online.
- Children know the meaning of the term ‘phishing’ and are aware of the existence of scam websites.
- Children can explain what a digital footprint is and how it relates to identity theft.
- Children can give examples of things that they wouldn’t want to be in their digital footprint.

Resources

Unless otherwise stated, all resources can be found on the [main unit 4.2 page](#). From here, click on the icon to set a resource as a 2do for your class. Use the links below to preview the resources; right-click on the link and ‘open in new tab’ so you don’t lose this page.


- Set the 2Respond Activity SPAM as a 2do for your class. However, change the Title and Description before you set it as follows:



The screenshot shows a window titled 'Set 'SPAM' as 2do'. It contains the following fields and controls:

- Title:** A text box containing 'Email Practice'.
- Description:** A text box containing 'Let's revise what you know about 2Email.' with a small icon on the right.
- Audio instructions:** A red circle and a grey play button icon.
- Set date:** An empty text box.
- Hand in date:** An empty text box.
- Enter a tag:** A text box.
- Next:** A purple button.

This is an Email simulation of SPAM messages, at the end of each message is a line that says ‘*Email Simulation 2Respond activity’. You can make this activity more realistic by editing the simulation to remove this reference if you wish. Go to Tools>2Email>2Respond Creator. In the search bar of the screen that opens, type ‘Spam’. Click on the result and then ‘Open Selected’. You can then edit any of the messages in the thread by clicking on them on the left-hand side.



When you are happy with the contents, save the file and then click on the  button and set the activity as a 2do.

- SMART rules displayed in the classroom or as screensavers or backgrounds on devices. Resources to do this can be found in the Teacher area in [Online Safety Resources](#).
- [Digital connections 2Connect file](#), save a copy of this file in the class folder and enable collaboration by clicking on this button  ().
- (Optional) set the 2Respond activity Confidential Information as a 2do.



Activities

1. Instruct the class to open the 2do that you set. This should take them to their 2Email inbox with a mail waiting for them called 'ATTENTION - Don't delay replying'.
2. Tell them you have to sort something out for a few minutes, while you are doing this, they should check any mails that they have and respond to them if necessary. The text of the first message is:

Dear Customer,

You have been selected to enter our prize draw. You are a guaranteed winner.

Please press reply and type in *winner*.

Bob - Global Email Company.
*Email Simulation 2Respond activity

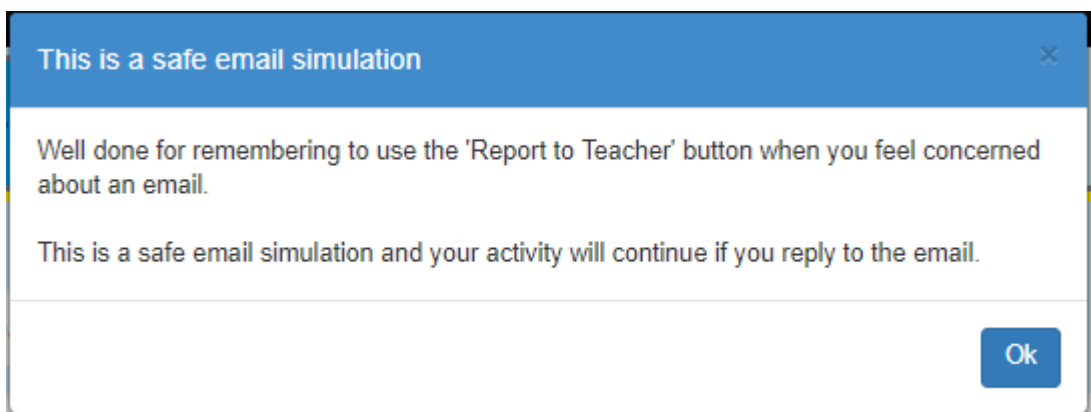
3. See how the class react, some will realise that it is a simulation, some will not. Some will report the message, and some will reply to everything. The details of the rest of the simulation are as follows:

Subject	Contents
Apply today to receive your free gift	<p>We recently sent you an email regarding a prize draw. We thought you might also be interested in a free gift.</p> <p>Instructions on how to claim your free gift will be sent to you if you reply to this email stating you would like a free gift.</p> <p>Kind regards,</p> <p>Bob - Global Email Company. *Email Simulation 2Respond activity</p>
Tick tock - time is running out!	<p>Dear Customer,</p> <p>We would like to inform you that a special offer is available to you. We have 200 gold watches which have to be given away free. Every single watch just has to go by next week. Don't delay and reply today!</p> <p>Yours sincerely,</p> <p>Bob - Global Email Company Customer Manager. *Email Simulation 2Respond activity</p>
URGENT Get your money back by replying today!	<p>Dear Customer,</p> <p>Do you fancy some cash in your pocket? Are you tired of having to save up to buy the things you want?</p>



	<p>Now you can get 50% of your money back you spent this year in shops and online stores.</p> <p>Reply YES to get this amazing unbelievable offer.</p> <p>Yours sincerely,</p> <p>Bob - Global Email Company Customer Manager. *Email Simulation 2Respond activity</p>
<p>SMART PHONE FOR YOU</p>	<p>Dear Customer,</p> <p>Due to our warehouses being so full up with smart phones we have decided to give some of them away. YOU have been selected to receive a free smart phone.</p> <p>Please press reply if you wish to receive the latest smart phone completely free.</p> <p>Yours sincerely,</p> <p>Bob - Global Email Company Customer Manager. *Email Simulation 2Respond activity</p>
<p>ALERT - SPAM!</p>	<p>Dear 2Respond user,</p> <p>I hope by now you have carefully thought about the SMART rules and the importance of following them. Remember to never ACCEPT emails from unknown senders or organisations.</p> <p>Not only is SPAM annoying to get but it can be very harmful to users and can even spread computer viruses.</p> <p>Take care,</p> <p>Cyber Cop</p>

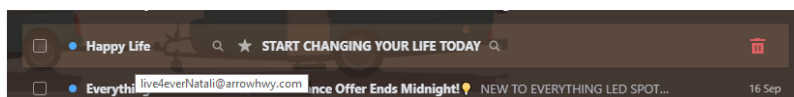
If children click on the Report to Teacher button, they are informed that they have done the right thing but also given the chance to complete the simulation. They will see this message:





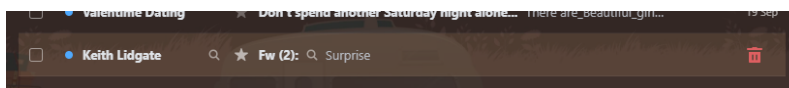
4. Once children finish the task ask them to find out the SMART rules; you can direct them to the resources, they will need to report them back to the class.
5. Talk about the simulation. What features indicated that this was SPAM? Which of the SMART rules would protect you from such mails? (S-safe, A-accepting, T-tell).
6. What are the implications of giving the personal information that the emails were requesting? Go through each mail:
 - ATTENTION - Don't delay replying' - Replying to the first mail shows that the email address is in use; SPAM sending is often done by computer programs that send out thousands of messages at a time, just by responding, you are giving an indication that you could be exploited. What should you do? - Report and put in spam folder.
 - Apply today to receive your free gift - The second mail has an attachment; should you open attachments from unknown sources whose reliability you don't know? What could the attachment do? It could put a virus on your machine that obtains your private information or damages the device.
 - Tick tock - time is running out! - The third mail is a 'too good to be true' mail, if something seems too good to be true then it is probably a scam.
 - URGENT Get your money back by replying today! And SMART PHONE FOR YOU – More too good to be true mails. They would request personal details and even bank details to send you the 'gifts'. These would never arrive but you would have given away details that people could use illegally.
 - Things to watch out for in real-world email is the email address that the mail comes from. It might look like it comes from a proper company but when you click on the details of the email address it will be made of nonsense words or not the address that you would expect.

Note for teachers; look in your personal email spam folder for any examples that you can show the class. Here are some examples:

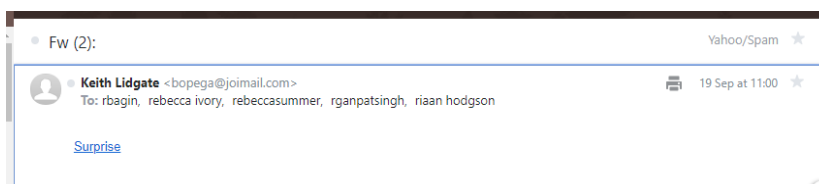


Look at the email address in the pop-up

This one is supposedly from a friend called Keith Lidgate, but the title is unusual, it looks like he's forwarded it maybe.



opened the mail:




No text, just a link to click and it's not his usual email address. Hover over the link and the page it takes you to appears in the status bar at the bottom of the screen:



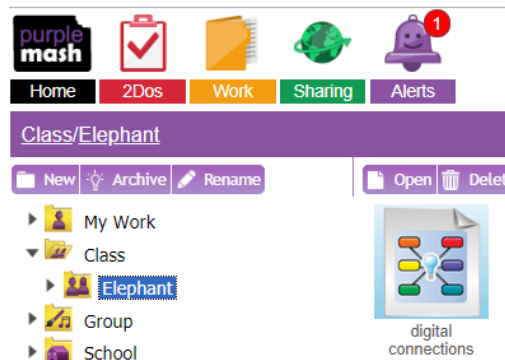
travel
madinina4x4.com/gpuyyje/9mc7uh=Keith_Lidgate

This doesn't look like a familiar site. It's almost definitely Spam. If in doubt and you know the person, email them on their **usual email address** to check, maybe they have had their email used in identity scams themselves.

If you click on a link that could be genuine and it is asking for personal information you can also check for the padlock symbol in the address bar of your Internet browser. This indicates a site that uses software to make your connection with them secure, so details cannot be intercepted:

 <https://www.purplemash.com/>

7. These types of emails that are trying to get your personal details are known as phishing scam emails; they are 'fishing' for information about you that they can use.
8. Ask the class if they remember what a digital footprint is? If they have followed the scheme, they will have learnt about this in year 2. If they need a reminder then you can use the quiz **from the year 2 unit [Digital Footprint Quiz](#)**. Go through the questions together. In year 2 children were learning about how to keep their identifying details safe. They learnt that a digital footprint is a permanent record of your online activities.
9. Is a digital footprint a bad thing? Children might say that it is, but it is only bad if the things that you share or that are shared about you, reflect badly upon you and project and image of yourself that you don't want people to see. Or if putting the information together could affect your personal privacy and security.
10. Open the [2Connect file Digital Connections](#) on the whiteboard. This shows possible things that might be part of a person's digital footprint. Clicking on a node will open further notes about the item. Ask children to open the same file from their class folders. To do this, they need to click on the Work tab and then on the little arrow next to 'Class' on the left-hand side then click on their class name. They will see the file Digital Connections to open. Children should add to this and colour-code to show positive and negative pieces of a footprint. The yellow nodes are people who might look at your digital footprint.



11. If time allows, or if you wish to follow this up for homework, children could complete the Confidential Information 2Respond activity using their improved knowledge of online safety and digital footprint influence to advise someone else.



Lesson 2 – Beware Malware

Aims

- To Identify the risks and benefits of installing software including apps.

Success criteria

- Children can identify possible risks of installing free and paid for software.
- Children know that malware is software that is specifically designed to disrupt, damage, or gain access to a computer.
- Children know what a computer virus is.

Resources

Unless otherwise stated, all resources can be found on the [main unit 4.2 page](#). From here, click on the icon to set a resource as a 2do for your class. Use the links below to preview the resources; right-click on the link and 'open in new tab' so you don't lose this page.

- Set the 2Respond activity 'Downloading Software' as a 2Do for your class, as in the previous session, change the name of the activity to 'Waremal Virus Update' and the description to 'Email installation practice'.
- [Malware slideshow](#); to use on the whiteboard.
- Set the [Online Safety Top Tips](#) as a 2do for the class

Activities

- Review the SMART messages from last week; refer to the posters that you used.
- Ask children to complete the 2Respond activity. After having done 2Respond tasks last week, they are likely to work that this is a simulation. Ask them to use the activity to give you some information about what installing something could do to a device.
- These are the emails in the Downloading Software thread:

Subject	Contents
FW: URGENT: Update your virus protection now!	<p>Hi,</p> <p>I just received the mail below, please read it. Do you think I should have followed these instructions? I'm a bit worried now.</p> <p>from Jamie.</p> <hr/> <p>Dear Customer,</p> <p>This mail is from your Internet Service provider. A virus has been detected on your computer</p> <p>Please press reply and type in download. You will get a message that a file is being downloaded and you can safely ignore it. You might get warning messages from your virus software. It is safe to disable the software and download this program.</p> <p>Bob - Global Email Company.</p>



	*Email Simulation 2Respond activity
Oh, dear what have I done?	<p>Hi,</p> <p>Things have gone really strange on my computer; programs keep popping open asking me to input my details. I can't close them so I've emailed you from my mum's phone. She doesn't know my computer has gone wrong.</p> <p>I searched for a virus help app on her phone and found something free from our usual virus protection company, should I download it onto her phone and see if it can help me?</p> <p>I'm panicking a bit now.</p> <p>from Jamie.</p>
Trying to be sensible!	<p>Hi,</p> <p>I realised that even though that is a reputable app, it won't help me to fix my computer and I shouldn't install things on my mum's phone without her knowing. It was asking me to share her login details.</p> <p>What should I do?</p> <p>from Jamie.</p>
Thanks for your advice	<p>Hi,</p> <p>Thank you for your advice I remembered the SMART rules and decided the best thing was to TELL. So I told my mum and she has managed to turn the proper virus protection back on. She ran a scan and it removed a virus from my computer.</p> <p>She says it's very good that I didn't have any important logins saved on my machine as the virus could have shared them with people.</p> <p>I'm only going to install things if I've checked with a trusted grown-up now.</p> <p>from Jamie.</p>
ALERT - SPAM!	<p>Dear 2Respond user,</p> <p>I hope by now you have carefully thought about the SMART rules and the importance of following them. Remember to never ACCEPT emails from unknown senders or organisations.</p> <p>Not only is SPAM annoying to get but it can be very harmful to users and can even spread computer viruses.</p> <p>Take care,</p> <p>Cyber Cop</p>



4. Go through the slideshow together.
 - Slide 1) How do you know if a download is safe?

If children have downloaded something, how did they determine it was safe?

- Apps; you can download some apps without going through a well-known app store such as Apple, Amazon or Google Play, this is riskier. Though even through a recognised Appstore, you can end up downloading apps that ask for access to all your personal details such as phone contact and ability to change files on your device.

- Slide 2) What is Malware?
- Slide 3) AdFly

When downloading on a PC, you often get taken on a journey through lots of confusing adverts; Minecraft mods are notorious for taking you on this journey. It can be really hard to work out where to click to get what you want, and you can end up downloading things that could be harmful by mistake.

- Slide 4) what is a computer virus. At this point discuss the WannaCry virus; you might be able to find a video about the effects of this online. Discuss the impact of such an attack; it could mean a life or death situation to patients.
 - Slide 5) HTTPS and security certificates – activity look inside the padlock.
 - Slide 6) Cookies – activity.
5. Children can now begin work on the Online Safety Top Tips 2do. This should be comic book style to grab people's attention. Each box could contain a character and speech bubble giving advice about one of the areas that children have been learning about. In summary, these are:
 - Phishing and spam
 - Identity theft
 - Digital footprint
 - Malware
 - Computer virus
 - Secure websites and cookies
 6. They can then add to this document in the next session which is about plagiarism.



Lesson 3 – Plagiarism

Aims

- To understand that copying the work of others and presenting it as their own is called 'plagiarism' and to consider the consequences of plagiarism.
- To identify appropriate behaviour when participating or contributing to collaborative online projects for learning.

Success criteria


- Children are able to determine whether activities that they undertake online, infringe another's copyright. They know the difference between researching and using information and copying it
- Children know about citing sources that they have used.

Resources

Unless otherwise stated, all resources can be found on the [main unit 4.2 page](#). From here, click on the icon to set a resource as a 2do for your class. Use the links below to preview the resources; right-click on the link and 'open in new tab' so you don't lose this page.

- [Completed Writing Template about Tim Berners Lee](#). This file contains two pages, the first is plagiarised, the second is not. This will be used as a whiteboard resource.
- Access to Wikipedia
- [Plagiarism Quiz](#)
- Print the [Screen-Time Record Card](#). Each child will need a copy (each sheet has two record cards and can be cut in half), this is to hand out at the end of the session for children to complete over the week in preparation for the next lesson.

Activities

1. Open the Tim Berners-Lee example on the whiteboard. Look just at the Early Life section on the first page.
You will need to zoom in using the  button. What do children think of the content? Why are there bits in different colours and numbers on it? What is the purpose of the writing on the photo? Why do you think it is there? (It is called a watermark and indicates that the picture is copyrighted).
2. Click on one of the links, where does it take you (Wikipedia), why do they think this happens?
3. Scroll down to the second page and compare the two versions. Which is better and why?
4. Compare the Career sections for both. Which contains better information?
5. Search for Tim Berners-Lee on Wikipedia in a separate tab of your browser and compare this to the two homework examples. Children should notice that the first example is simply copied and pasted into the template whereas the second uses the information, but it is rewritten.
6. The first version is plagiarised from Wikipedia. Does anyone know anything about plagiarism? Plagiarism is when a person steals another's work and claims that it is their own. You can copy things in some contexts, such as quoting another person or using an image or video but you must give credit to the original author: This is called 'citation'.
7. There are clues that teachers use to tell whether someone has plagiarised work. The first will be to search the same theme online. Comparing the second version about Tim Berners-Lee to the Wikipedia version you can see that the writer has looked up and explained terms. For example, the meaning of 'inaugural' in



the awards section or what MIT is. They have filtered out some of the information to make it appropriate to the reader.

8. In the second version the writer has cited the sources for the image used and for the source of their information (underneath the image and at the bottom of the page)
9. Discuss where the line lies when participating or contributing to collaborative online projects for learning.
 - If you share a collaborative 2Connect file that the class made on your own blog, what should you do?
 - If you and a friend create a poster and then you enter it into a competition as your own individual work, is that correct?
 - If you find a piece of work in the class shared folder that you like. Can you open it, change it and call it your own work?
10. Split the class into 2 or 4 groups to do the plagiarism quiz. If a team gets the question correct, they chose their 'team colour'. Select a different question for the next question (otherwise the answer is too obvious!).
11. Hand out the record-card to be completed for the next lesson (ideally in a weeks' time). Discuss how to fill in the cards. Children should record how much time they spend on screen, which device and what they were doing as well as off-screen activities that they do.



Lesson 4 – Healthy Screen-time

Aims

- To identify the positive and negative influences of technology on health and the environment.
- To understand the importance of balancing game and screen time with other parts of their lives.

Success criteria

- Children can take more informed ownership of the way that they choose to use their free time. They recognise a need to find a balance between being active and digital activities.
- Children can give reasons for limiting screen time.
- Children know what to do to report on distressing or inappropriate things that they come across online.

Resources

Unless otherwise stated, all resources can be found on the [main unit 4.2 page](#). From here, click on the icon to set a resource as a 2do for your class. Use the links below to preview the resources; right-click on the link and 'open in new tab' so you don't lose this page.

- Completed record cards handed out in the end of the last session.
- [Screen-Time 2Investigate Database](#). You should save this in the shared class folder in Purple Mash but do not set the database to be collaborative yet.
- [Screen Time Study writing frame](#) to be set as a 2Do.

Activities

1. Ask children to look at their record cards and to work out the following:
 - The total screen time for the week in minutes.
 - The total non-screen time activity in minutes.
 - Which day had the most screen time
 - Which day had the least screen time.
 - Average hours of sleep per night (you might have to show children how to calculate this).
2. Ask them to (privately) consider whether they think they have the right balance between screen time and other activities.
3. Open the Screen-Time Database on the whiteboard. Explain that the 2Investigate database can be used to collect everyone's information easily. Each child will be creating their own record of data. Click






on the Design Database button to look at what the record will contain. Each question is called a 'field' of the database. This one contains the following fields:

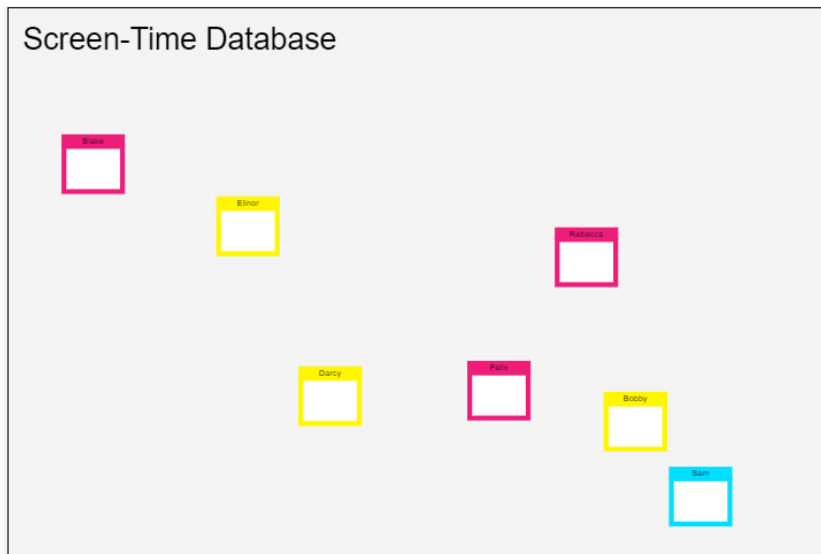
- Screen time and activity time in minutes; as previously calculated.
- Screen-based activities; at this point, click on the pencil button for this field. You will see that there is list of activities. Ask children for any other required activities to include here and add them. Children should select the main activity they do.
- Highest/Lowest screen-time day, children will select which day they had the lowest or highest screen time.
- Control of screen-time; this is a yes/no question. If children's screen time is controlled by adult intervention or timers or a timetable.
- Average hours of sleep per night


1	First name		
2	Total screen time (mins)		
3	Total activity time (min)		
4	Activities done on screen		
5	Highest screen time day		
6	Lowest screen-time day		
7	Is your screen time controlled		
8	Average hrs of sleep per night		
9	Experienced upsetting content?		

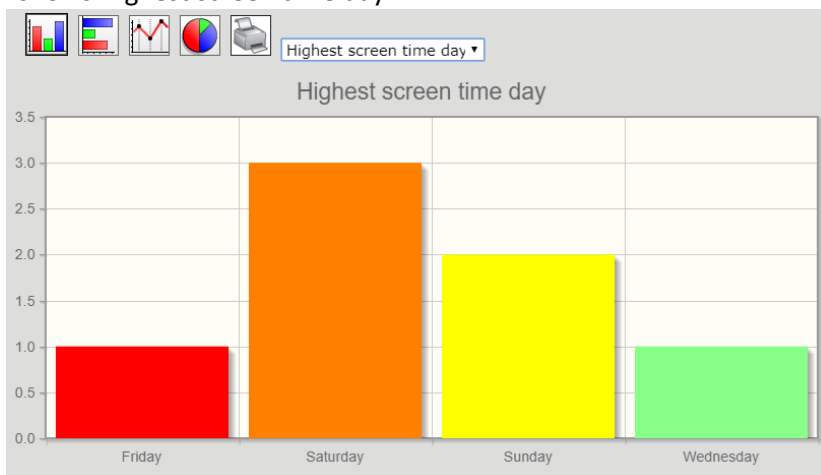


- Experienced upsetting content; this is a yes/no question. If they have ever been upset by something online, they should answer yes.

- Once you are happy with the record structure, click the collaboration button . You might be prompted to save again, then the button should indicate the database is now collaborative: .
- Children should open 2Investigate on their own devices. They should then click on the Add Record button  and input their details. For Data Name, children can use their first name (you could anonymise this by giving each child a letter or random word to insert if you wish).
- The database should update in real-time on the whiteboard. When all children have input their data, it will look something like this:



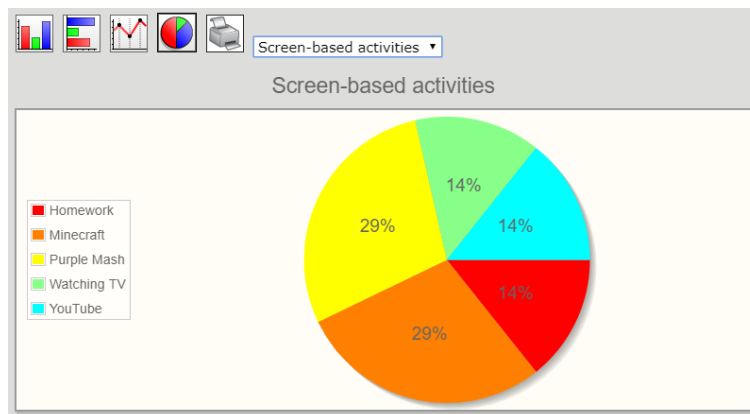
- Now try making some graphs to find out about the class' screen time information. Click on the Charts button . On the Charts screen, you can select the field to examine in the drop-down box, the example below shows Highest screen time day.



- You can also create different types of charts using the buttons at the top, this example shows a pie-chart of the different on-screen activities.



9. Use your class' results to discuss how they feel about the amount of screen time they have in relation to the amount of time spent on other activities. Discuss the following:
- Positive and negative influences of technology on their education, on their physical health, on mental wellbeing, on the environment.
 - Sleep time. Look up the recommended hours of sleep for children of their age and compare this to the data; does screen time take away sleep time? What happens to their screen a night?
 - Can they suggest reasons to balance screen-based activities with other activities in their life and what will prevent them from doing so; temptation, peer pressure, used to a routine, financial, weather, etc.
 - Do they see screen-time restriction as a bad thing imposed on them or can they see why such restriction is in place in some households?



10. Show children how to take a screenshot of a graph. The method will be device dependent. On a PC use the Snipping Tool and then save the image to the computer. On an iPad click the home button and the off/on button at the same time. The image will save to the Photos app and can then be cropped if needed. On many Android tablets, click the off/on button and volume down button at the same time, then crop the image which will be found in the Gallery.
11. Ask children to create one of the graphs on their own devices and then to save. They should then open the writing frame set as a 2do and insert their graph into the picture box on the writing frame (using the green up arrow).
12. Before completing the writing frame, turn to the last question about upsetting content. You might wish children to share what sort of things they have seen or experienced and your response will depend upon their experiences. The important teaching point is to give children the knowledge of what to do in this situation. Discuss:
- Applying the screenshot technique to save any upsetting messages that they receive to save evidence to show an adult.
 - How to report upsetting content within an app e.g. the Report to teacher button in 2Email
-
- and report buttons in online platforms.
- Who to talk to if anyone or anything upsets them online.
13. They should complete the writing frame recording the class discussion and their opinions and strategies.



Assessment Guidance

The unit overview for year 4 contains details of national curricula mapped to the Purple Mash Units. The following information is an exemplar of what a child at an expected level would be able to demonstrate when completing this unit with additional exemplars to demonstrate how this would vary for a child with emerging or exceeding achievements.

Assessment Guidance	
Emerging	<p>Children contribute their ideas to discussion of spam email (lesson 1), malware (lesson 2) and plagiarism (lesson 3). They have included appropriate content in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). They have been able to share their work online.</p> <p>With support throughout, children show an understand what online safety is. In a small group, they can use 2Connect (Unit 4.2 Lesson 1. Point 3) to map out the key features of online safety. Children produce a simple leaflet, postcard or slideshow etc about online safety, which can then be used as part of presentation to parents (Unit 4.2 Lesson 1. Point 7).</p>
Expected	<p>Children have decided upon the most important online safety messages to communicate and have shared these ideas in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). They put this knowledge into action in their own online activity.</p> <p>Children can explore key concepts relating to online safety using 2Connect Unit 4.2 Lesson 1. Point 3). They help others to understand the importance of online safety (Unit 4.2 Lesson 2. Point 3) and apply their knowledge through the creation of online safety resources which are then used as part of presentation to parents (Unit 4.2 Lesson 1. Point 7).</p> <p>Using the example from lesson 1, children can give some examples of things to look out for in an email to ensure that it from a valid source an is not a phishing scam email. They can explain what can be learnt by looking at the padlock details for a website (lesson 1)</p> <p>Most children can reflect upon positive and negative aspects of a digital footprint and can give examples of the care they would take when sharing online in relation to their and others' digital footprint (lesson 1).</p> <p>Most children can give reasons for taking care when installing apps or software. They know what Malware is and the possible impact of computer viruses and can give recommendations for how best to ensure that they only install valid software as part of their top tips document in lesson 2.</p> <p>Most children can give reasons for limiting screen time that include the effect on physical and mental health. In lesson 4, they were able to reflect on their own screen time and collective class screen time and begin to make informed decisions about when to limit their own screen time.</p> <p>Most children can explain how plagiarism is stealing, they are beginning to be able to identify the aspects of sharing that would be classed as plagiarism (lesson 3)</p> <p>In lesson 4, children were able to include actions for reporting cyberbullying or inappropriate content in their screen time study document.</p> <p>By completing lesson 4, most children would have saved both online and locally to a device and are able to explain the differences between the two storage types.</p> <p>Most children will be able to identify key messages that should be shared with other children and parents about online safety, including identification of reliable content from websites found via common search engines (Unit 4.2 Lessons 1 & 2).</p>



Assessment Guidance

Exceeding	<p>Children have decided upon the most important online safety messages to communicate and have shared these ideas in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). Children demonstrate that they are making connections between the positive possibilities that technology provides e.g. collaboration and sharing and the possible downsides of this such as malware and phishing. They actively use this knowledge to support their own online activities safely.</p> <p>Children demonstrating greater depth understand the key concepts and implications of the choices they make relating to online safety (Unit 4.2 Lesson 1. Point 3). They help others to understand the importance of online safety (Unit 4.2 Lesson 2. Point 3) and apply their knowledge and approach to staying safe online in all areas of the curriculum (Unit 4.2 Lesson 1. Point 7).</p>
-----------	--