



**Newall Green
Primary School**

Aiming High To Reach Our Goals

Firbank Road, Newall Green, Wythenshawe, Manchester, M23 2YH
Tel: 0161 437 2872 Fax: 0161 436 2178 www.newallgreen.manchester.sch.uk



E-Safety Policy

Document Control	
Title:	E-Safety
Date:	May 2023
Supersedes:	Version 3
Related Policies / Guidance:	ICT policy Behavior policy Code of Conduct SEN Policy Equality /Inclusion Policy Pupil Privacy Policy Preventing radicalization and risk assessment policy Safeguarding Whistleblowing Staff Code of Conduct
Review:	May 2024 –or if sooner if needed

Approved by:	Governors	Date: 30.11.23
Last reviewed on:	May 2023	
Next review due by:	May 2024	

The E-Safety policy applies to all members of NGPS (including staff, students / pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports.

Andrew Wild is the named *E-Safety Governor*. The role of the *E-Safety Governor* will include:

- *regular monitoring of e-safety incident logs that are logged on CPOMs*
- *reporting to relevant Governors / Board / committee / meeting*

Head teacher and Senior Leaders:

- **The *Head teacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**

- **The *Head teacher* and the members of the Behaviour monitoring team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.**

- *The Head teacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*

- *The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*

Behaviour monitoring team

- Responds initially (Cyber Bullying, down loading inappropriate information) to the incident and informs the Head teacher.

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- liaises with the Local Authority / relevant body
- liaises with school technical staff
- current issues are addressed through the report to Governors for behaviour & safety.

Healthy Schools team / ICT focus group

- provides training and advice for staff on how to prevent incidents & what to look out for
- keeps up to date with current guidance and trains staff
- monitors the curriculum coverage of the pupils to ensure e-safety is delivered

Network Manager / Technical staff in conjunction with the Head Teacher, are responsible for ensuring that:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**

- that the *school* meets required e-safety technical requirements and any *Local Authority / other relevant body E-Safety Policy / Guidance* that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
 - that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Principal / Senior Leader; E-Safety Coordinator*

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current *academy* e-safety policy and practices
- they have read, understood and signed the Code of Conduct that outlines the acceptable use
- they report any suspected misuse or problem to the *Head teacher* for investigation / action / sanction
- all digital communications with parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
 - in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2. Child Protection / Safeguarding Including PREVENT.

Every member of staff must take responsibility to ensure that pupils are not put into a position where serious child protection / safeguarding issues could arise from such as:

- sharing of personal data
- access to illegal / inappropriate materials or materials that may radicalise an individual (**Prevent Duty**)- see school code of conduct
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- if any staff see something they are not happy with please report to a senior member of staff – Whistleblowing Policy.

Pupils: will be taught what ‘acceptable use’ through the scheme of work is. They will be able to demonstrate that they have:

- a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school’s* E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature*. Parents and

carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users will not be able to access the school's systems but may be able to use the internet and will follow this policy whilst doing so.

3. Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum we use is broad and relevant. It provides progression, with opportunities for creative activities and will be provided in the following ways:

- **The e-safety curriculum is planned through regular ICT lessons and as part of Computing / PHSE / other lessons.**
- **The Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices

Parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, website,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications*

Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **ICT training is given to all teachers and TAs on a rolling programme for curriculum content & e-safety advice.**
- **At the start of the year or as a new member of staff joins the team the member of staff will sign the code of conduct which explains the acceptable usage policy & also the member of staffs role in e-safety throughout school.**
- *The Healthy School Team provide regular updates and information to train staff as new information becomes available – this information is sourced from Manchester's Healthy Schools team.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*

Governors

Governors take part in e-safety training / awareness sessions so that they are able to fulfil their role in Keeping Children Safe in Education.

Training will take place in school where appropriate or on line. It will cover up to date issues that link the children's safety to electronic device usage such as 'Prevent', bullying, grooming, etc.

- Participation in school training / information sessions for staff

4. Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that staff and children within school follow the policy and procedures.

- **School technical systems are managed to ensure the school meets recommended technical requirements**
- **Servers, wireless systems and cabling are securely located and physical access is restricted to areas where staff only have access.**
- **All users will have clearly defined access rights to school / academy technical systems and devices.**
- **The ICT focus group are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.**
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

5. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**

- **Transfer data using encryption and secure password protected devices.**

6. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Mobile Devices

Aims:

To ensure mobile devices are not misused by pupils, school personnel, parents and school visitors.

To ensure the safe and acceptable use of mobile devices.

To ensure compliance with all relevant legislation connected to this policy.

To work with other schools and the local authority to share good practice in order to improve this policy

We recognise personal communication through mobile technologies is an accepted part of everyday life and we acknowledge that we have a duty to ensure that mobile phones are used responsibly at this school.

We understand parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety and that it gives parents the reassurance that they can contact their child instantly. We believe children should not bring their mobile phones into school with the intention to be used on school grounds during the school day. We feel that mobile phones can cause disruption in lessons, the possibility of theft, loss or damage and also the possibility of child protection issues. Therefore, we require a child, who brings their phone into school, to then hand it into the school office or to the class teacher immediately on their arrival. Once handed into their class teacher, the teacher will then secure the phone in a secure box, locked in a secure room/cupboard. Parents will be contacted immediately if a child breaks this rule and will be asked to collect the mobile phone from the school office.

We believe parents and all school visitors have a responsibility not to use their mobile phones on school premises for the making or the receiving of phone calls and especially for the taking of photographs unless in the case of an emergency.

During the school day school personnel are also restricted on the use of their mobile devices, for further information see school social media and acceptable use policies. These can be found www.newallgreen.manchester.sch.uk.

However, school personnel's phones will remain switched on for health & safety reasons eg: if on the field and there is an urgent need to contact them. It is the responsibility of all school personnel to keep their mobile phones securely stored. School personnel are not allowed to use their own personal phones to take pictures of children

Images – safe use of images

Taking of images and film digital images are easy to capture, reproduce and publish and, therefore, easily misused.

We must remember that it is never appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.

However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and immediately deleted from the staff device.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on field trips.

Publishing pupils' images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- General media appearances,
- local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire school year once the planner and consent form page has been filled in, unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Where two parents have legal responsibility for a child, consent has to be given by them both in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa.

Storage of Images

Images/ films of children are to be stored on the school's secure network.

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

E-Safety

Use of the school's ICT equipment by any members of the school community including parents/carers and visitors must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

The Importance of Internet use in Education

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Using the Internet to Enhance Learning

The school Internet access will be designed expressly for student use and will include filtering. Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

The need for students to learn to evaluate online content.

If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Head of School.

The school ensures that the use of Internet derived materials by staff and by students complies with copyright law.

The Management of Chat Rooms

Students will not be allowed access to public or unregulated chat rooms.

Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised by staff.

E-Safety Guidelines

The main reason we provide internet access to our teachers and pupils are to promote educational excellence by facilitating resource sharing, innovation and communication. However for both pupils and teachers, internet access is a privilege and not an entitlement. The school will take all reasonable precautions to restrict pupil access to both undesirable and illegal content.

Whole School Network Security Strategies

The uploading and downloading of non-approved software is not permitted.

All access to the school network requires entry of a recognised user ID and password. Pupils must log out after every network session.

Regulation and Guidelines

The school's internet access incorporates a software filtering system to block certain chat rooms, newsgroups and inappropriate websites. The aim of this is to achieve the following:

- Access to inappropriate sites is blocked
- Access will be allowed to only a listed range of approved sites
- The content of web pages or searches is filtered for unsuitable words
- A rating system is used to rate web pages for inappropriate content and that web browsers are set to reject these pages
- Records of banned sites visited by pupils and teachers are logged.

Email

Pupils may only use their approved email accounts on the school network. Access in school to external, web-based, personal email accounts is denied for security network reasons. It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender.

Pupils may not reveal their own or other people's personal details, including passwords, addresses or telephone numbers, or arrange to meet someone out-side school via the school network.

Pupils are given information on E-Safety during PSHE lessons and dedicated ICT lessons.

See full policy at: <http://newallgreen.manchester.sch.uk/files/ict-e-safetypolicy.pdf>

E-safety Prevent

The internet provides children and young people with access to a wide-range of content, some of which is harmful.

Extremists use the internet, including social media, to share their messages. The filtering systems used in our school block inappropriate content, including extremist content.

We also filter out social media, such as Facebook. Searches and web addresses are monitored and the ICT technician will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Where staff, children or visitors find unblocked extremist content they must report it to a senior member of staff.

We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones.

Cyberbullying

Students are taught about the proper use of telecommunications and about the serious consequences of cyber-bullying and the school will, through PHSE and in ICT lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.

The school trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. The school block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present.

GUIDANCE FOR STAFF

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Go with the pupil and see the Head of School

Computers

- Ask the pupil to get up on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Accompany the pupil, taking the offending material, to see the Head of School
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour in accordance with the behaviour policy and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

The Management of Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. If this does happen it must be reported immediately.

Current online trends/apps

Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online world.

The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks. Children are taught through the PSHE and ICT curriculum about staying safe online and are taught to think about the positives and negatives of being online as well as the potential impact on mental health and wellbeing. Newsletters and information for parents/carers is regularly shared to make them aware of how to help their child stay safe online as well as the age restrictions and dangers associated with current online trends and apps.

Informing Students

Rules for acceptable use will be posted in all rooms where computers are used.

Students will be informed that Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access.

Maintaining the ICT System Security

The school ICT systems will be reviewed regularly with regard to security.

Virus protection will be installed and updated regularly. If a member of staff leaves then all administrator level usernames and passwords will be deleted.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. Andrew Wild is the named E-Safety Governor. The role of the E-Safety Governor will include:

- regular monitoring of e-safety incident logs that are logged on CPOMs
- reporting to relevant Governors / Board / committee / meeting

Head teacher and Senior Leaders

- The Head teacher will ensure that monthly internet usage checks are carried out by the ICT technician and reviewed for misuse of internet.
- Will ensure that data is stored following the principles of the GDPR policy.

Network Manager

- Will ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Will ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed and are encrypted.

Use of digital and video images

- Staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Communications

A wide range of rapidly developing communication technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies and clearly states what is allowed and not allowed.

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons				✓	✓			
Use of mobile phones in social time	✓				✓			
Taking photos on personal mobile phones / cameras				✓			✓	
Use of school devices	✓					✓		
Use of personal email addresses in school, or on school network		✓			✓			
Use of school email for personal emails	✓				✓			
Use of messaging apps for school purpose	✓				✓			
Use of social media for school purpose	✓				✓			

ICT Acceptable usage (AUP)

Children

ICT Acceptable Use - AUP is outlined in the home school diary

Keep yourself safe, keep the internet fun

During school, teachers will guide pupils towards appropriate materials on the internet. Outside of school, families bear the same responsibility for such guidance as they engage with information on the TV, telephone, movies, radio and other potentially harmful media.

Please see <http://ceop.police.uk> for further guidance.

In order for your child to be allowed access to the internet at school you must complete the permission form below.

Pupil (to be completed in school)

As a school user of the internet, I agree to comply with the school's rules on its use. I will use the internet in a responsible way and observe all restrictions explained to me by the school.

Pupil Signature:

Parent / Carer (this section must be completed in order for access to the internet to be granted)

As the parent or legal guardian of the pupil signing above, I grant permission for my child to use electronic mail and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable or age inappropriate and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.

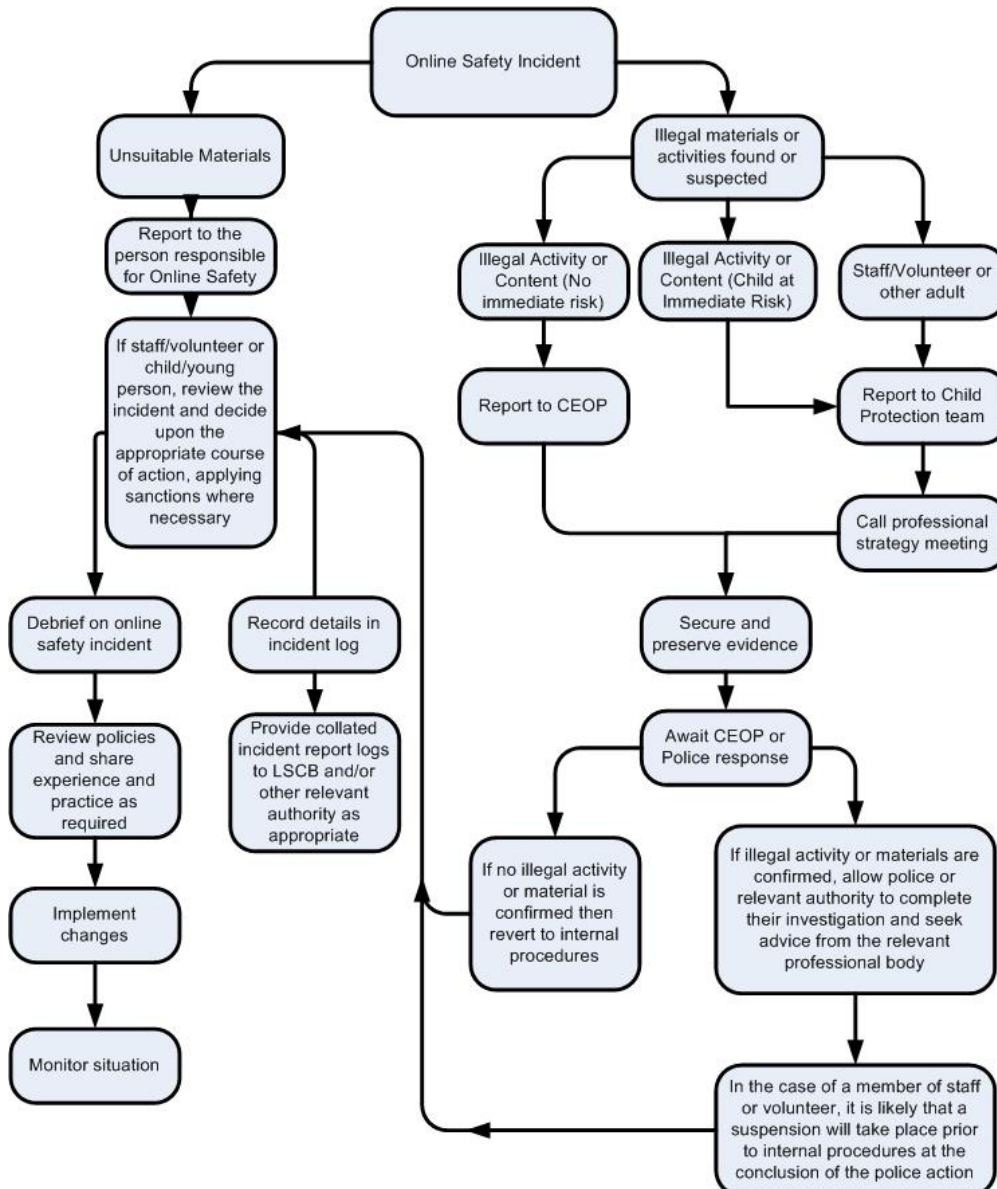
Parent / Carer Signature:

Staff

This should be read in conjunction with the School's Staff Social Media and IT Acceptable Use policies. These can be found www.newallgreen.manchester.sch.uk

Responding to incidents of misuse

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

School Actions & Sanctions

Student/pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email	X				X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

[Accessing learning from home](#)

[Home Learning](#)

Whilst we endeavor to have all our students back in school and class, we understand that some families and children have circumstances that currently make this unviable. Home learning will be provided for children from families who are identified as high risk.

Families entitled to this service will be dealt with on an individual needs basis.

[Virtual Learning](#)

Once the families who need support are enrolled, the child or children will be required to be present for their virtual learning in order to receive their attendance mark for each individual day.

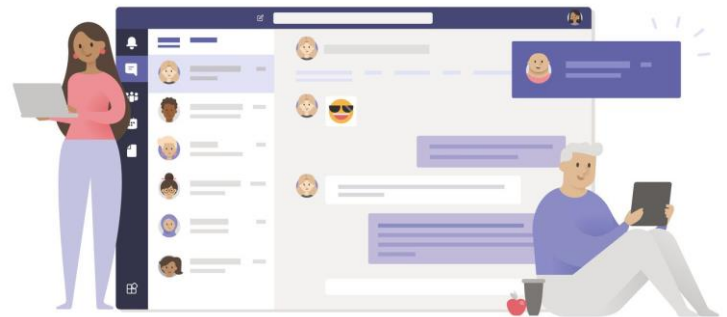
Each day your child or children are learning virtually, they will be expected to complete the following tasks:

- Attend two interactive, online meetings with their virtual learning teacher to receive input, support and feedback.
- Complete the assigned activities before the end of the school day.
- To be active and online during school hours in case further support or clarifications of misconceptions are needed.

[Virtual learning platform](#)

Microsoft Teams

We use Microsoft Teams for all our learning from home needs.

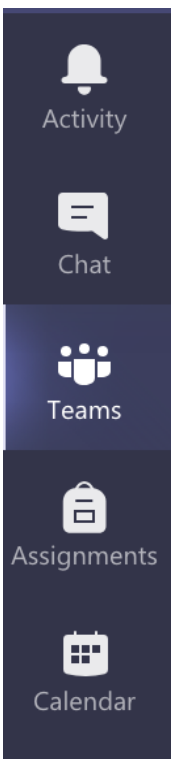


Each child will be provided with their own account which is restricted from any services unsecure for them. Children will be unable to create group meetings or communicate with others therefore this tab (to the left) will be restricted.

The Teams tab permits children to enter their class for group discussion, files of work, updates and assignments.

Work will be found on assignments. Here you can update and edit work, review previous work and see feedback given.

Children will have their own calendar of meetings on this tab. Here children are expected to attend meetings, twice daily.



Other applications to further education

As a school, we aim to support and facilitate learning wherever possible. In order to continue to provide the best provision for our children, we have different services to encourage, reading, spelling and numeracy for use in school, during lessons but also at home.

Each of the following applications require a username and password. Usernames and passwords are available from your child's class teacher.

Spelling Shed



Times Table Rockstars



Reading Eggs



Tapestry

Tapestry is an application used in school to create online learning journals for each individual child. Once a new child is enrolled into our school you will receive the following letter:



You will have received an activation email from Tapestry which you can set up your own password to login with. You will also be asked to set up a 4-digit PIN which you can use on the Tapestry app to quickly log back in once you've initially logged in. Do remember to keep an eye out on your spam/junk folders for this email.

Tapestry allows you to login with a secure username and password so you can view all your children's observations, photographs and videos. You can like and comment on observations that we add for your child and it's also possible for you to add your own observations. Your comments and own observations will allow us to find out about which activities your child really enjoyed and the learning they get up to at home. In The event of a class having to isolate for 2 weeks we will be using it as our virtual learning platform to communicate with you.

It's also possible for you to be notified via email either immediately, daily or weekly if there are new entries for you to view.

All data that is entered to Tapestry is stored securely on their servers. If you are interested in finding out more information about this, you can go to <https://tapestry.info/security>.

Once we have set you up with an account you will be able to login using any web browser from tapestryjournal.com or by downloading the Tapestry app from the Play or App store, depending on what type of device you are using. Remember, if you are going to use the App version of Tapestry to ensure auto updates are turned on for your device so you always have the most up to date version of the app.

Here is a link to a help video to talk you through it.

<https://www.youtube.com/watch?v=n7ROkDnb4I0&list=PLthyVDX1AWQJeGUqAna3ZEhEqbgidx0Yt>

If you have any problems accessing your Tapestry account contact the school on 0161 437 2872 and ask for Sophie Tait. I will help solve the problem.

When you log into **Tapestry** you are agreeing to the following terms:

- As a parent I agree I will not publish or share any observations, photographs, voice notes or videos from the online learning sessions on any social media site.
 - As a parent I agree that communication with the teacher is solely to support my child's learning and is done so in a professional manner.
 - I understand that some teachers may have to work at home so responses to questions sent may not be immediate.
 - I understand the need to keep all who use online learning safe and I have read the NGPS – keeping children safe online information which can be found on the website.

Tapestry for Parents and Relatives: Web Browser Version Guide

Note on Terminology: 'Setting' is a term meaning Newall Green Primary School

Where to find Tapestry

To access the web browser version of Tapestry go to www.tapestryjournal.com or follow [this link](#) if reading a digital version of this guide. You can also use a setting-specific link that staff at your child's setting may have given you. Tapestry does not have high system requirements, but please make sure you update your web browser to the latest version available for the best user experience.

Login Information

In order to use Tapestry, your setting will have to create a user account for you on the system.

Tapestry support (the customer services team) are unable to create or modify relative accounts; if you have an issue with your Tapestry account please contact your setting. Tapestry support can only directly provide parents and relatives with basic advice on how to use the system.



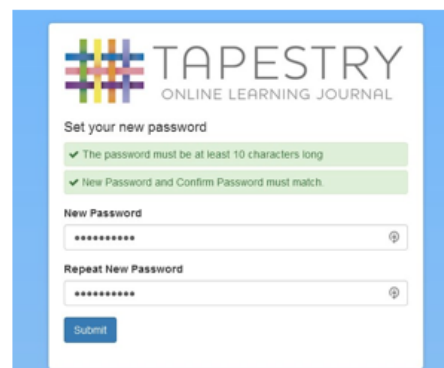
The screenshot shows the Tapestry login interface. At the top is the Tapestry logo and the text 'TAPESTRY ONLINE LEARNING JOURNAL'. Below this are two input fields: 'Email address' and 'Password', both with masked characters. A blue 'Log in' button is positioned below the password field. Underneath the button, there is a link that says 'Having trouble logging in?'. At the bottom of the form, there are two buttons: 'Need help? Tapestry Tutorial' and 'New to Tapestry? What is Tapestry?'.

Your Username: This will be the email address your setting used to register you on Tapestry, for example jparent@example.co.uk.

Your Password:

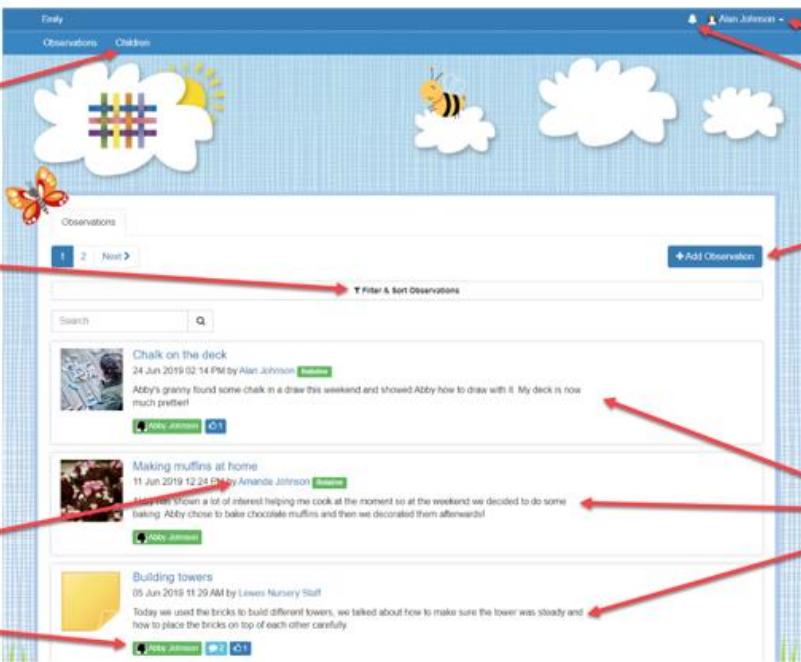
You will receive an email generated by your setting that contains a link you can follow to set up your own password and PIN number for Tapestry. This link will expire 30 days after it has been sent. If your link has expired or won't work for another reason, please contact your setting manager for assistance.

You can change both your email and password through the browser version of Tapestry whenever you like.



The screenshot shows the 'Set your new password' page. At the top is the Tapestry logo and the text 'TAPESTRY ONLINE LEARNING JOURNAL'. Below this is the heading 'Set your new password'. There are two green checkmark messages: 'The password must be at least 10 characters long' and 'New Password and Confirm Password must match'. Below these are two input fields: 'New Password' and 'Repeat New Password', both with masked characters. A blue 'Submit' button is at the bottom left of the form.

Tapestry Browser Version Interface: Observations Screen



Children Tab: This takes you to the profiles of the children you are linked with

Filters: Use these to refine what appears on this list. E.g. Observations with pictures, including comments etc

Author of the Observation

Child's Name

Your Username

Notifications

Add Observation: Use this button to add an observation

Observations: These are the observations made for your child. Click the title or picture to view the observation in full

Your Username

Access this drop-down menu by clicking on your username in the top right of the screen

Your Downloads: Here you can access observations/pictures/videos if the setting have made them available to download

Edit Preferences: From here you can change your email, password, PIN and notification settings

Log out of your account

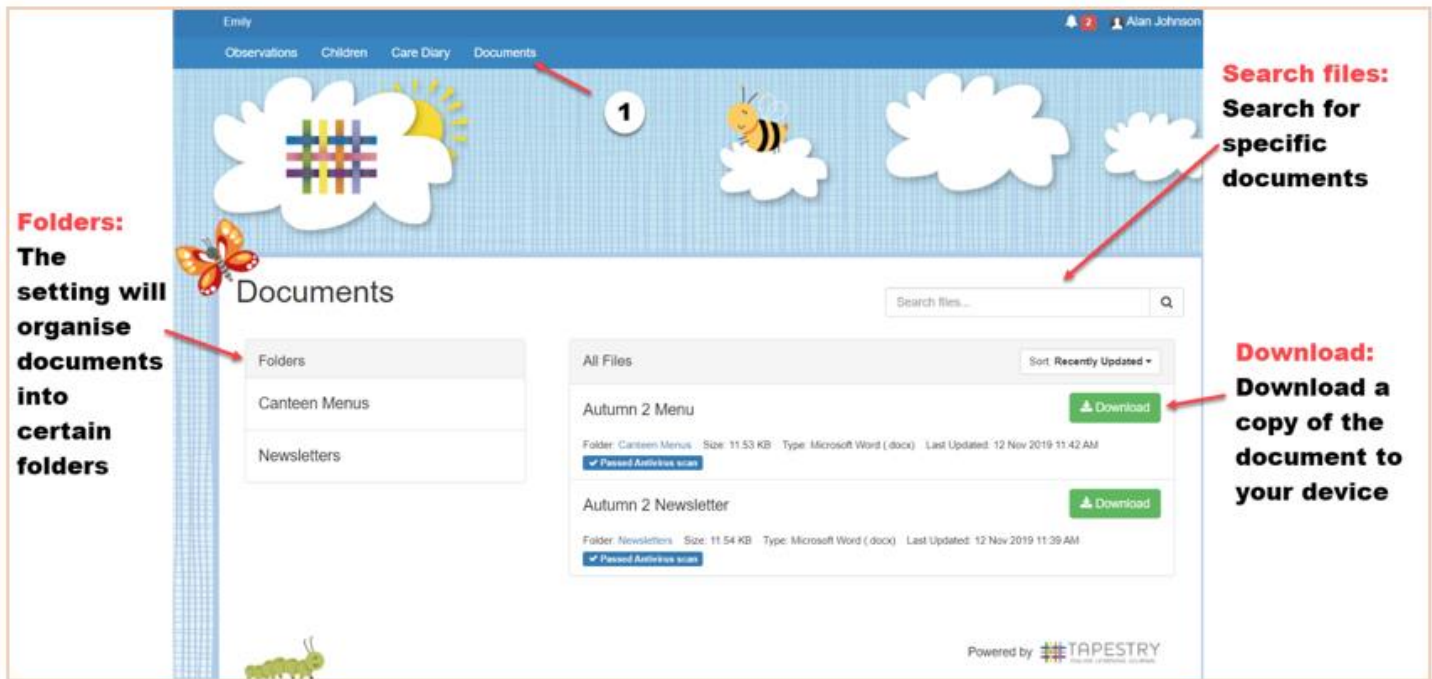


Help and Tutorials: Contains a link to Relative Tutorials and your setting's relative contact email address

OPTIONAL: Documents

The setting may upload documents to Tapestry and make them available for you to view and download.

In order to do this, click the “Documents” tab on the homepage (1)



Folders:
The setting will organise documents into certain folders

Search files:
Search for specific documents

Download:
Download a copy of the document to your device

Emily
Observations Children Care Diary Documents

1

Documents

Search files...


All Files Sort Recently Updated

Autumn 2 Menu [Download](#)

Folder: Canteen Menus Size: 11.53 KB Type: Microsoft Word (.docx) Last Updated: 12 Nov 2019 11:42 AM
[View Password Protected](#)

Autumn 2 Newsletter [Download](#)

Folder: Newsletters Size: 11.54 KB Type: Microsoft Word (.docx) Last Updated: 12 Nov 2019 11:39 AM
[View Password Protected](#)

Powered by  TAPESTRY
ONLINE LEARNING JOURNAL

Monitoring Engagement with Remote Education

It is important that children engage with the remote education provided so that they don't fall back with their learning, however we do acknowledge that each family's home circumstances are unique and there may be factors that affect engagement with home learning. These may include parents working from home or with limited access to technology, amongst other factors.

Communication is essential and we would ask that if there are circumstances that mean a child cannot engage at least partially with the remote education that their parent speaks to the teacher. We can then work together to find a means of providing remote education that works for that family's circumstances.

Acquiring technology and technological support

Equipment loans

To access learning from home, children will require a suitable device: mobile phone, tablet, laptop or a computer. If this is not available to you please ask for a "loaned" device.

- Must be returned at the end of isolation
- Only used for educational purposes

Technological support

Technology is continuing to evolve at a very quick pace. We understand that parents/carers may feel apprehensive or uncertain on how to support their children through the use of technology. For support with applications, internet or equipment, first speak to your child's class teacher. If they are unable to help, they will refer you to the ICT Co-ordinator, who can arrange tutorials of support.

Internet Access

To access learning from home, children will require internet access.

If families do not have internet at home or access to the internet, the school are able to provide families with a code – through a partnership with BT – to access free Wi-Fi. This free Wi-Fi is subject to accessibility in your area and availability due to limited codes.

Home Learning Contingency Plan

DFE expectation	Teachers will provide in the event of a bubble isolation or school closure			
	EYFS	KS1	Lower KS2	Upper KS2
How will parents/ pupils know how to use the on-line platform for learning?	Will use Tapestry – teachers will send an explanation of how to use the platform.	A guide will be available on the website with simple instructions for using Microsoft Teams. This can be translated into other languages with the translation tool available on the website.		
How many lessons will be prepared?	A daily timetable will be shared with the children & Parents – this will outline the lesson details. Each Year group has a Newsletter & Knowledge Organiser explaining the Topic overview for the Term – the timetable will link to this.			
How many lessons per week?	<p>5 Literacy lessons – For Nursery Nursery Rhymes, Phonics and either one story revisited or a daily story. For Reception Phonics activities that include the above as appropriate with the addition of a writing element. 5 Maths lessons; Based on the teaching that was planned for class teaching. Reading – either Reading Eggs or an appropriate reading task set so daily reading takes place. Topic- practical tasks that can be completed to develop children’s physical or artistic skills. Well-being / PHSE on-line safety information</p>	<p>5 Literacy / 5 SPAG / 5 Reading tasks. Teacher led input followed by independent task. Possible resources Oak Academy, Pobble 365, BBC, 5 Maths tasks Teacher explanation – then independent task</p> <p>Non-Core Subjects Activities that follow the timetable that can either be a practical activity – such as a link to a Physical challenge such as The Body Coach/ art activity/ research activity Or a written response / quiz to check understanding</p> <p>Well-being / PHSE Time on-line with peers for a group chat PHSE curriculum planned activities On-line safety information Children will be asked to keep a worry journal / or to email their teachers with concerns using Microsoft Teams.</p> <p>Tasks may be a pre-recorded voice over a PowerPoint presentation / a link to a website such as BBC or Oak Academy / a pre-recorded lesson – your child’s class teacher will decide the best way to share the information.</p>		

How will you collect the children's response to task?	Parents collect responses and keep until the children have returned after 14 days or use Tapestry to share response to a task.	The pupils can up-load their work to Microsoft Teams Work can be dropped off at the School Office to be marked by a member of staff.
How will children with no access to ICT complete their work?	<ol style="list-style-type: none"> 1. Please let us know if you are unable to access on-line learning as we may have a device you can borrow. 2. A work pack can be picked up from the Office and returned on a weekly basis that covers the same materials as those learning on-line. 3. Parents please remind children that the work set is not optional – they will need to complete the daily tasks to ensure they do not fall behind their friends. 	
How will teachers feedback their comments?	<ol style="list-style-type: none"> 1. For those children accessing Microsoft Teams – feedback sessions are planned into the daily timetable. 2. For those handing in tasks – marked work and feedback will be available to collect as the next pack is picked up from the Office. This may only be a comment as we would want to keep the pieces of work to be stuck in the child's class book. 3. We may provide a mark sheet so you are able to help your child mark their own work. 	
How often will my child see a teacher on-line?	We ask that you help your child to meet their Teacher on Tapestry daily – the teacher will inform you of the times.	Your child will be required to be on-line once a day with the class teacher as long as the class teacher is well enough to undertake this role. The teacher will sort out the exact times with your child as they plan the weekly timetable. The on-line session will set and explain the tasks for the day's activities.
What do I do if I need paper / pens etc for my child to complete their work	Resources can be collected from the School Office following the Covid distancing guidelines & the wearing of face coverings / masks.	

Online safety at home

We all care about what our children are doing online.
We want to use technology to have fun using the internet.
We all want to act safely and responsibly.

