E-Safety Policy

Remote Learning for Future Lockdowns.

E-Safety Policy - Remote Learning for Future Lockdowns.

This document has been written as an appendix to the existing safeguarding and E-safety policies based on the most recent government guidelines available on 31/08/2020 for Remote Learning and E-Safety during school closures or local lockdowns. The reviewing of this policy will be on-going as and when the government guidelines change.

At Our Lady Star of the Sea Primary Catholic Primary School, we recognise that we are currently experiencing unprecedented times in the continued response to the Covid-19 crisis.

As a school we recognise that during these times children's schooling may need to return to remote learning during local lockdowns or periods of self-isolation for 'bubbles'. We also note that this means during these times, children may be spending a lot more time online to access remote learning. We therefore recognise that now, more than ever, it is extremely important that we ensure a safe online learning environment and that our staff, children and their parents/carers are aware of current guidelines and available support for E-Safety concerns.

Remote Learning Precautions:

Safeguarding Leads will:

- Ensure all websites given to children are secure and follow school monitoring programs
- Ensure all staff are monitoring children's use of games/websites/remote learning sites provided
- Monitor and act upon any online safety concerns reported by staff
- Ensure all apps/websites/logins are GDPR compliant and age appropriate
- Offer advice to parents if contacted regarding online safety via p3501.admin@durhamlearning.net
- Referrals to social care and or police if needed regarding an E-Safety concern.

Teachers will:

- Ensure all websites given to children are secure and follow school monitoring programs
- Continue to follow schools E-Safety guidelines and procedures and monitor children's usage
- Continue to follow safeguarding policies in reference to concerns about a child and report these appropriately to a safeguarding lead.
- Continue to look for signs that a child may be at risk online during remote learning.
- During any contact with parents/carers reinforce and model guidelines on keeping children safe online and appropriate internet usage.
- Continue to educate children on appropriate and safe internet use, modelling good practise of online communication peer to peer and teacher to pupils.

E-Safety Policy - Remote Learning for Future Lockdowns. Apps/Websites for Remote Learning

As a school we have asked the children and their families to use the following website for interactive remote learning using their log in details provided.

- Office 365-Teams
- Lexia
- Times Tables RockStars
- Numbots
- Fiction Express
- Spag.com
- EdShed

We have also given a further list of recommended websites in home learning packs for example BBC bitesize, Phonics Play and many more which do not require the children to have personal login details during these times.

Prior to assigning these websites and tasks all staff have ensured they are:

- GDPR compliant
- Age appropriate and accessible
- Fit within school monitoring systems e.g Smoothwall
- At Our Lady Star of the Sea Primary we are using Office 365 and Teams as a means of communicating with parents/carers and children.

Leaders have:

- ✓ ☐Ensured Office 365 and Teams is GDPR Compliant
- ✓ ☐Set up using a strong password
- ✓ ☐Ensured this is a link to parents, and children should not access this on any personal account or login.

When using Office 365 and Teams staff will:

- Only access Office 365 and Teams for communication on a **school device** (laptop or iPad).
- Follow school's acceptable usage policy when using Office 365/Teams.
- Continue to follow schools E-Safety guidelines and procedures and monitor children's usage
- Continue to follow safeguarding policy procedures in reference to concerns about a child and report these appropriately to a safeguarding lead.

As a school we have set up Office 365 –Teams for all children to allow virtual teaching where appropriate and remote learning.

Office 365 Teams will be used for:

- ➢ Virtual whole class lessons/small group meetings.
- ➢ Use teaching tools to support learning such as assignments, interactive, messages, announcements and whiteboards etc.

Leaders have:

- Ensured Office 365 Microsoft Teams is GDPR Compliant
- Set up Microsoft Teams using a strong password
- Gained parental consent for each child using Microsoft Teams
- Authorised this policy and its expectations.
- Ensured this is a link to parents, and children should not access this on any personal account or login.

When using Office 365 Teams staff will:

- ➢ Only access Microsoft Teams for communication on a **__school device__** (laptop or iPad).
- ➢ Follow school's acceptable usage policy when using Microsoft Teams
- ➢ Microsoft Teams live lessons must only take place during school contact hours (8.30-4pm).
- ➢ Continue to follow schools E-Safety guidelines and procedures and monitor children's usage
- ➢ Continue to follow safeguarding policy procedures in reference to concerns about a child and report these appropriately to a safeguarding lead.
- ➢ Monitor children's usage and ensure children only access Microsoft Teams services such as messaging and video calls when requested to do so for educational purposes.
- ➢ Ensure children's parents/carers are aware in advance and at the present time that a live virtual lesson or meeting is taking place to ensure appropriate use.
- ➢ Avoid 1-1 meetings to safeguard children and teachers (if needed consult EHT first for approval).
- ➢ Ensure live lessons are taught and accessed from a natural place/background in the home—no bedrooms for children or staff.
- ➢ Ensure live lessons or video calls are secure and not open to public.

At Our Lady Star of the Sea Primary when a child is using Microsoft Teams we expect parents to:

- ➢ Educate children on appropriate use of the site.
- ➢ Monitor children's use ensuring it fits with this policy and acceptable internet use.
- ➢ Ensure children are not accessing services on Teams such as messages or live video calls or lessons by themselves.
- ➢ Support children in effective and appropriate use of this site for education purposes.

E-Safety Policy.
Reporting and Advice.

At Our Lady Star of the Sea Primary Catholic Primary School we advise the following websites, based on Government guidelines (31/08/2020) for reporting concerns and advice. The following will be shared with parents/carers.

Reporting routes for children during school closures (age appropriate):

➢ CEOP-https://www.ceop.police.uk/safety-centre/
➢ Child Line
https://www.childline.org.uk/?utm_source=google&utm_medium=cpc&utm_campaign=UK_G O_S_B_BND_Grant_Childline_Information&utm_term=role_of_childline&gclsrc=aw.ds&&gclid =EAIaIQobChMIlfLRh-ez6AIVRrDtCh1N9QR2EAAYASAAEgLc-vD_BwE&gclsrc=aw.ds
➢ UK Safer Internet Centre https://reportharmfulcontent.com/

Reporting routes and advice for parents/carers:

➢ CEOP-https://www.ceop.police.uk/safety-centre/
➢ Internet Matters
https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYA SAAEgIJ5vD_BwE
➢ London Grid for Learning https://www.lgfl.net/online-safety/default.aspx
➢ Net Aware https://www.net-aware.org.uk/
➢ Think-u-know https://www.thinkuknow.co.uk/
➢ Parent info https://parentinfo.org/
➢ UK Safer Internet Centre https://www.saferinternet.org.uk/advice-centre/parents-and-carers
➢ NSPCC Parent Advice: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Alternatively, you can contact the school or your child's class teacher directly, with any concerns regarding online safety and reporting an issue.

E-Safety Policy.

Acceptable Use Teachers

Office 365 & Teams:

Please make sure you have read and understood the information and guidance in this policy, as well as the poster below from National Online Safety.

Staff must not record live lessons at any time. National Online Safety Guide;

https://nationalonlinesafety.com/guides/10-top-tips-remote-learning-for-teachers

National Online Safety: Teams Tips

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

Microsoft Teams, or simply 'Teams', is a platform that allows for collaborative working, either as students or as professionals, using communication capabilities through audio, video and instant messaging. The software is available both online through a web browser and to download from microsoft.com. Users can have 1:1 online meetings or set up live events to host up to 10,000 people. Groups can be set up to include only relevant users and almost all file-types can be uploaded and shared, from PDFs and Word documents to audio and video files.

AGE RESTRICTION 13+

What parents need to know about MICROSOFT TEAMS

DISCLOSING PERSONAL DETAILS

Like any messaging service or social network, children can be targeted by others to share their private or personal information ranging from their phone number, birthday and home address to their social media accounts or even their personal login details and passwords. Oversharing their private information can lead to any manner of risks including online fraud, bullying or even grooming activity.

CYBERBULLYING

The risk of cyberbullying can be increased online when using chat facilities. Microsoft Teams provides the ability for users to chat to each other via its instant messaging service, both as part of a group or privately. Children can find themselves the target of negative or hurtful comments directed from other users who might find it easier to say things they maybe otherwise wouldn't in person.

#BULLY

INAPPROPRIATE CHAT

The chance to have private conversations in Teams can also mean that children feel as though they can share messages and communication between each other that are hidden away from others. Whilst children are most likely to use Teams in a school setting, the ability to chat privately may provide an opportunity to be less formal which could lead to sharing inappropriate messages, files or content which is unsuitable in a school environment.

HACKING RISK

Teams, like any software application, may be a target for hackers to illicit personal data. A 'man-in-the-middle attack' could occur, whereby the attacker reroutes communication between two users through the attacker's computer without the knowledge of the other users. This means that online communications could possibly be intercepted and be read or listened to, exposing both parties to the possibility of identity fraud or other criminal behaviour.

VIRUS INFECTION

Viruses and other harmful programs are among the risks of using online platforms like Microsoft Teams. Wherever you can share files or links, there is a risk that the content could be malicious. This could lead to slow computer performance, deletion of data, the theft of private or personal information and even hackers taking control of your PC.

LIVE STREAMING RISKS

Microsoft Teams, like other video-conferencing software platforms, facilitates live streaming. That means it inevitably carries some of the associated risks. These are likely to be minimal within a controlled environment (for instance in a classroom setting / remote learning). However, live streaming means that content isn't always moderated and children may inadvertently view or hear inappropriate, unsuitable or offensive material that they otherwise wouldn't.

Safety Tips for Parents & Carers

NOS National Online Safety
#WakeUpWednesday

BLOCK USERS

If your child is receiving inappropriate messages or finds themselves being harassed or abused on Teams, they can block these contacts from the privacy control in the settings menu. To add an extra layer of protection, you can also block contacts whom hide their ID to protect children from communicating with people they don't know.

BLOCK

PROTECT PERSONAL INFO

It's a good idea to talk to your child about the importance of keeping their personal information private and secure. Children should only give out the minimum information they need to when creating an account and understand that if other people request their personal details from them, they should avoid providing it and report any concerns to a trusted adult.
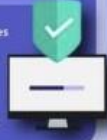
ENABLE BACKGROUND BLUR

To help protect your privacy during a video call or live stream, it may be a good idea to blur the background or even add a background effect. This can easily be done by clicking 'Background effects' before joining a meeting after which you'll have the option to blur your background, replace your background with one of the images provided or upload and use an image of your own.

UPDATE COMPUTER SECURITY

It's important to ensure you perform regular computer and software updates, as these patches often improve security flaws and minimise your vulnerability to cyberattacks. Having your own computer security or anti-malware software is another level of defence in minimising the chances of an attack from viruses, malware and other harmful programs. Ensure this is updated everyday so that it is able to protect you against the very latest threats.

TALK ABOUT RISKS

As a parent, talking to your child and making them aware of the risks of working and communicating online can help them to be more digitally resilient. Perhaps outline a set of agreed do's and don'ts and try to ensure young people know what to do if they are made to feel uncomfortable or experience any negative behaviour or activity.

AVOID VIDEO/AUDIO

It's always a good idea to turn off your audio during live group calls when not in use. This can easily be done by muting the mic and will avoid others hearing anything personal in the background at home or at school. Similarly, if possible, try to encourage children to avoid using video call to help guard against any privacy concerns and limit the risks of viewing anything inappropriate or unsettling.

SOURCES:
https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/group-chat-software
https://www.microsoft.com
https://www.thinkuknow.co.uk

Meet our expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

Dear Parents/Carers,

As a school we recognise the importance of continued education and support for children during the current lock down. Therefore, as a school, and in line with Department for Education guidance, we have set up Office 365 for all students. This will allow access to Microsoft Teams. As a school, we are keen to have all children taking part in the live lessons on Teams. Teams is now also being used for sharing Word, feedback and announcements. We have also set up Teams to allow direct messages to the teacher. This is to support the communication with parents whilst the children are learning at home. However, we must highlight that this part of Teams is only for parents, children **must not** use the messaging service to communicate with the teacher or anyone else.

Your child will be given their own username and password. Please ensure your child uses this site safely and in line with the school policy attached to this letter. Please take some time to read the information about the new set up, and your child's safety and learning on it, and our expectations of acceptable use as a school detailed in this policy. If you have any questions, please ask your child's class teacher. Make sure you keep the email address and password safe as this will be needed to access the site each time.

We also recognise that this means during these times, children may be spending a lot more time online to access remote learning. We therefore recognise that now, more than ever, it is extremely important that we ensure a safe online learning environment and that our staff, children and their parents/carers are aware of current guidelines and available support for E-Safety concerns. General E-safety tips can be found on our school website and we encourage you to monitor your child's screen time and usage and to share any concerns with their class teacher.

We really appreciate the support provided from yourselves and the children during the previous remote learning period and we hope you will continue to work with us to keep all of our children learning during these times.

Thank you

E-Safety Policy.

Acceptable Use Children/Parents

Parents

- ➢ Make sure you supervise your child at all times whilst they are working remotely, on a live lesson or accessing online resources.
- ➢ When on a live lesson, make sure children are in a communal room in your house, appropriately dressed.
- ➢ Children must not access Teams without the teacher present, this means they must not use it as a chat-based site between friends. They should only attend Teams when a meeting has been scheduled by the teacher.
- ➢ Monitor children's screen time and usage and report any concerns to your child's teacher.
- ➢ Live lessons should not be recorded at any time.

Children.

- ➢ Treat remote learning as you would classroom learning, make sure you take regular breaks, particularly from your screen.
- ➢ Make sure you are looking smart and focused for a lesson, and make sure your grown-ups are helping you to access Teams.
- ➢ Only access and work on websites/games/online tasks that your teacher has asked you to do.
- ➢ Do not share any passwords or personal information online.
- ➢ If you are worried about something online, tell your grown-ups!

Remember Teams is for learning, not talking to friends!

You MUST NOT access the 'messaging' service on Teams.

Children should only access Teams for a live lesson when the teacher is present or to retrieve an assignment.

National Online Safety Guide;

https://nationalonlinesafety.com/guides/10-top-tips-remote-learning-for-children

https://nationalonlinesafety.com/guides/10-top-tips-remote-learning-for-parents

National Online Safety®
NOS
#WakeUpWednesday

REMOTE EDUCATION
10 TOP TIPS FOR PARENTS

Remote education ensures continuous learning outside the classroom. For parents and carers, remote education isn't always straightforward and there can be a number of factors they need to consider, especially around ensuring their children feel comfortable and are familiar with the whole concept. That's why we've created this guide to help parents and carers support their child in getting the most out of their remote education experience.

1. TAKE AN ACTIVE INTEREST IN YOUR CHILD'S LEARNING

As a parent or carer, your school may have explained how remote education works already, but children may still need help. Take an active interest in their learning and help support them whenever they need a helping hand.

2. MONITOR YOUR CHILD'S COMMUNICATION AND ONLINE ACTIVITY

It's important to remind your child that despite being at home, the same level of behaviour and conduct exists as if they were at school. Encourage them to remain polite, remember their manners and not to post or send any negative comments just because they are behind a computer.

3. ESTABLISH A DAILY SCHEDULE AND ROUTINE

Working from home and trying to learn in a more casual setting that children might associate more with play and a degree of freedom might take a bit of getting used to. Try to stick to a daily routine and use the timetable/schedule that schools have sent home to help children keep on top of their daily learning.

4. ENCOURAGE SCREEN BREAKS AND PHYSICAL ACTIVITY AWAY FROM DEVICES

Remote learning will inevitably require more interaction with computers, laptops and tablets. Teachers will invariably advise on screen breaks; however, it doesn't hurt to keep a check on their time online or encourage them to get some fresh air/exercise.

5. ENSURE YOUR LEARNING DEVICE IS IN PUBLIC SPACE IN THE HOME

It's important to consider where your PC or laptop is placed if live video is being used. Try to keep the background neutral, with no personal information visible and move learning devices out of the bedroom as this could be deemed inappropriate.

6. IMPLEMENT SAFETY CONTROLS AND PRIVACY RESTRICTIONS ON APPS AND SOFTWARE

Dependant on how your school implements remote education, your child may be required to download certain software or apps. Whilst these are likely to be relatively safe to use, like any other new app or platform, parents should still implement safety controls as a precaution.

7. ENSURE YOUR CHILD ONLY USES OFFICIAL SCHOOL COMMUNICATION CHANNELS

It's important that all communication with teachers and school staff is directed through approved school channels, whether that be through the school's online portal or the relevant secure messaging site.

8. FAMILIARISE YOURSELF WITH RELEVANT SCHOOL POLICIES

Schools should have a policy on remote education that they can share with parents. Familiarise yourself with this and ensure you know what is expected of teachers and your child during lessons, both online and offline.

9. MAINTAIN FEEDBACK WITH TEACHERS

Engage in communication with teachers where possible, and try to feed back progress and development as well as any helpful suggestions around the learning process. Be transparent but remain professional and only use official channels to communicate.

10. MONITOR YOUR CHILD'S WELLBEING AND MENTAL HEALTH

Remote education will likely mean that your child won't get the same level of social interaction and might not see their friends for a while. Keep a check on their wellbeing and try to encourage them to get out as much as they can. Whilst learning from home might seem fun and exciting to start to with, missing out on seeing their friends every day might take its toll.

At Our Lady Star of the Sea Primary Catholic Primary School we advise the following websites, based on Government guidelines (31/08/2020) for reporting concerns and advice. The following will be shared with parents/carers.

Reporting routes for children during school closures (age appropriate):

➢ CEOP-https://www.ceop.police.uk/safety-centre/
➢ Child Line
   https://www.childline.org.uk/?utm_source=google&utm_medium=cpc&utm_campaign=UK_G
   O_S_B_BND_Grant_Childline_Information&utm_term=role_of_childline&gclsrc=aw.ds&&gclid
   =EAIaIQobChMIlfLRh-ez6AIVRrDtCh1N9QR2EAAYASAAEgLc-vD_BwE&gclsrc=aw.ds
➢ UK Safer Internet Centre https://reportharmfulcontent.com/

Reporting routes and advice for parents/carers:

➢ CEOP-https://www.ceop.police.uk/safety-centre/
➢ Internet Matters
   https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYA
   SAAEgIJ5vD_BwE
➢ London Grid for Learning https://www.lgfl.net/online-safety/default.aspx
➢ Net Aware https://www.net-aware.org.uk/
➢ Think-u-know https://www.thinkuknow.co.uk/
➢ Parent info https://parentinfo.org/
➢ UK Safer Internet Centre https://www.saferinternet.org.uk/advice-centre/parents-and-carers
➢ NSPCC Parent Advice: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Alternatively, you can contact the school or you child's class teacher directly, with any concerns regarding online safety and reporting an issue.