

E-safety and Remote Education, January 2021

(Annex to E-Safety Policy available on the school website)

General statement of Intention

Over recent times, we have all developed our use of remote learning, largely through email and Teams as the primary platforms for our work. Keeping pupils and teachers safe during remote education is essential.

In reference to Keeping Children Safe in Education, 2020 (KCSiE), it is important to recognise the reference to Online Safety in Annex C: Online Safety. It is stated that *'The use of technology has become a significant component of many safeguarding issues...technology often proves the platform that facilitates harm.'* As such, we need to be mindful that with children spending increasing amounts of time using technology to access their work and working in greater isolation than normal, there is potentially greater risk of harm and we need to ensure that we have a clear policy in place that provides guidance to safeguard children and staff and offers guidance to parents and carers.

This annex sets out some of the considerations and approaches we are making in line with the changed arrangements in the school and following [advice from government](#) and local agencies. Even though this guidance was withdrawn in July 2020, the principles and practices of online safety for pupils and staff still apply. The annex also follows the government guidance on Safeguarding and Remote Education during Covid19 (updated Oct. 20)

Purpose:

The purpose of this annex to our existing E-Safety Policy and our Acceptable Use Agreements (for staff and pupils) is to provide a framework of guidance and safeguarding protocols to ensure that:

- children are safe during remote education.
- parents are informed of how to monitor and support the safety of their child.
- staff work within guidelines to protect them from allegations.
- children, staff and parents are aware of the appropriate reporting routes for any safeguarding concerns arising from increased use of remote learning

This document has been created in line with the DfE's Coronavirus (COVID-19):Safeguarding in schools, colleges and other provider's guidance (27th March 2020); guidance from Safeguarding in Education, Gloucestershire and Attendance in Education and Early Years Settings During the Coronavirus (COVID-19) Outbreak, updated on 12th January 2021. It has also been informed through reference to a wide range of other bodies, linked to issues around e-safety and listed in the appendix.

It is the responsibility of all members of staff to ensure that they are familiar with and adhere to this policy and understand the reporting routes and responsibilities in relation to any safeguarding concerns. (see also the School's E-Safety policy and Acceptable User Policies and the Annex to Child Protection Policy/COVID-19/Changes to our Child Protection Policy.)

Pupils and parents/carers will be sent details of the sections that are relevant to them and this full policy will be available on the school website.

1. Live Lessons

At Cirencester Kingshill School, we provide remote education using Microsoft Teams which largely follows pupils' usual school timetable. Based on [guidance from the UK Safer Internet Centre on safe remote learning](#), staff are aware that teaching from home is different from teaching in the classroom. Similarly, pupils (and their parents) know that learning from home is different to learning in the classroom. Teachers and pupils are encouraged to find a quiet or private room or area to engage in the educational process and are asked to note the guidance offered below.

2. Guidance for Staff: Remote Learning

- Teachers are asked that when delivering their sessions, they remind pupils of the need for appropriate conduct.
- Teams lessons are recorded, both to provide access at a later time for any pupils who may have missed the session or wish to review it, and also, if necessary, to ensure there is a record of anything that may be classed as inappropriate within our usual Behaviour Policy.
- An attendance record should be completed with issues around non-attendance followed up through communication with the pupil, parent, HoY and HOF, as appropriate.
- Teachers are asked to ensure that when delivering their sessions, they are professionally dressed and in a suitable workspace, remembering that this is visible to pupils. Background filters may be used to help achieve this.
- If online assessments are issued, it is important for teachers to reinforce the fact that these should be carried out independently and do what they can to reinforce the school guidelines.
- Teachers will contact parents and pupils where they are not accessing their Teams lessons and will inform Heads of Year if the situation does not improve.

3. Guidance for Staff: Communicating with Parents, Carers and Pupils

Whilst education is taking place remotely due to coronavirus (COVID-19), we must all ensure that we maintain professional practice as much as possible. When communicating online with parents and pupils, it is advised that staff should:

- communicate within school hours as much as possible
- communicate through the school channels approved by the senior leadership team, specifically email and the Show My Homework platform
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- do not share personal information
- Pupils will have weekly contact with both their Head of Year and Tutor. They will also receive updates regarding useful support services e.g. Teens in Crisis+ and how to access this.
- For pupils on the SEND register (regardless of whether they are in school or not), a key worker will make at least weekly contact, in a few cases this may be daily contact. This and any feedback including concerns raised, will be logged.
- The contact details of the DSL and Deputy are on the school web site so parents can contact should the need arise.

- Staff are also reminded of the need to take care not to share contact details when emailing multiple people and being careful when sharing usernames or other log-in details.

4. Providing Remote Pastoral Care

We are still able to provide a level of pastoral care remotely and as a school, maintain high levels of contact with pupils beyond the Teams lesson through weekly tutor sessions and Head of Year assemblies. We will ensure that every pupil has contact information for key members of staff so they know they can raise any concerns. This message is emphasised with pupils and with their parents through the Head's communication, Head of Year assemblies and tutor sessions run on Teams.

As well as this, staff within the pastoral and SEND teams act as key workers for our most vulnerable pupils, maintaining at least weekly contact. All staff are reminded that if calling a parent or pupil from their own phone, they should use 141 to withhold their number. It is preferable to call the pupil's home landline number or their parent's mobile number to speak directly to a pupil, but in the current time, we recognise that there are times when the parent may not be at home and there may not be a home landline so there may be occasions where a member of staff makes direct call to a pupil's mobile phone: this should always be done with the parent's permission.

5. Guidance for Pupils: Remote Learning

Whilst education is taking place remotely due to coronavirus (COVID-19), we must all ensure that, as well as making sure pupils keep up with their learning, they stay as safe as possible and adhere to the usual school expectations around appropriate behaviour. Guidelines to support their safety and to reinforce our expectations around pupils' conduct are outlined below.

- Pupils should try to maintain some structure to their day, following their usual school timetable through Microsoft Teams, as outlined above.
- They should also routinely check their school email and Show My Homework to keep themselves updated on communication from teachers and work that has been set.
- They should ensure that when accessing their lessons through Microsoft Teams, their cameras are turned off and they are on mute, unless requested to speak.
- Pupils must not record or take photos of classmates or teachers during Teams lessons, nor share lessons publicly.
- Pupils are advised not to forward any content within a Teams group – such as worksheets, examination papers, answers, solutions, videos, notes or links – to anyone else without the permission of the creator of that content.
- When encouraged to respond either through speaking or through using the Chat bar, they should do so: logging into the lesson in itself should not be the limit of their engagement!
- Pupils should complete the work that has been set and, if requested, send it into to their teacher, either through email or Show My Homework
- Pupils must remember that, despite being at home, a live lesson is an extension of the classroom and pupils should conduct themselves as they would at school. They should be responsible for their behaviour and actions when online, including ensuring that anything they type in the Chat

bar is appropriate and not liable to offend anyone else. They should always be polite and respectful to their teachers and fellow pupils.

- Pupils should understand that these rules are designed to help keep them safe online and that if they are not followed, school sanctions, where possible and appropriate, will be applied and parents contacted.
- If a pupil comes across offensive material they should report it immediately to their teacher or parent.
- Pupils are asked to communicate to staff through either Show My Homework, Microsoft Teams Chat facility or their school email account. They should not use any other email account for communicating with staff.
- Pupils should understand that all online activity is monitored. This includes anything on e-mail and in the Teams lessons.

6. Guidance for Parents, Supporting Engagement and Appropriate Conduct of your Child

- You should ensure that your child is checking in regularly for assigned work.
- When your child is watching a live lesson, you should try to ensure your child is in an area of the house that is quiet and free from distractions.
- It is important to remind children of their conduct online. As a member of Cirencester Kingshill School, they share a digital environment and their behaviour impacts the success of the online school community. Pupils must always follow the direction of their teacher just as in the classroom.
- Parents, pupils and staff are reminded that Microsoft Teams includes a chat function. It is important to note that this facility is monitored and sessions are recorded: pupils must be aware of the need to ensure that any chat is appropriate and not in any way, abusive or offensive to others.
- We would insist that students do not try to film the session using any device.
- Pupils are not to turn on their microphone unless the teacher invites them to do so. All microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to other participants.
- A live online lesson must be treated like a regular school lesson and only viewed by those who are invited to attend. The teacher will decide who should receive the invite through Teams. Only those invited by the teacher have permission to view the lesson.
- Cirencester Kingshill School does not expect any child to sign up to anything with a personal email address. They should either use their school email address or a username and password.
- Parents are asked to ensure that their child always keeps their login to both email and any educational software packages private and that they don't share their account with anyone.
- If online assessments are issued, it is important for parents to reinforce the fact that these should be carried out independently and do what they can to reinforce the school guidelines.

7. Online Risks

With all young people using the internet more during this period, we are aware of the signs and signals of cyberbullying and [other risks online](#) and as a school, we apply the same child-centred safeguarding practices as when children are learning in the school.

- The school continues to ensure appropriate filters and monitors are in place
- Our governing body will review arrangements to ensure they remain appropriate
- The school has taken on board guidance from the [UK Safer Internet Centre](#) on safe remote learning and guidance for [safer working practice](#) from the Safer Recruitment Consortium.
- Staff are reminded that professional boundaries must not slip during these unusual times and are reminded of the school's code of conduct and importance of using school systems to communicate with children and their families.
- Children and young people receive appropriate guidance on issues related to remote learning.
- Parents and carers have information via the website about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. Parents may find the links in the appendix helpful.

8. Safety Considerations for Parents (based on advice from [Nationalonlinesafety.com](#) and the [schoolbeat officer](#))

Secure online chats and chatrooms

It is normal for students to want to be able to communicate with each other whilst they are unable to see each other. It will help them feel less isolated and they will be able to help each other out with their home learning. When online, a child may also make use of chatrooms to get help on their work or to find someone to talk to. However, it is crucial that they can do this safely and there are also some risks associated with them, so it's important to reiterate general online safety advice around using messaging apps and chatrooms.

- Advise children to never give out personal information about themselves, friends or family online and always think before answering private messages.
- Ensure that your children don't put unnecessary personal information in the user profile of any apps that are installed for either educational or recreational purposes. For example, try to keep location, phone number and dates of birth private
- Some online 'friends' are actually just strangers and children should not hesitate to block people that make them feel uncomfortable. They should take a screenshot of their conversation if they need to report the conversation to someone.
- Children can always log out to avoid unwelcome situations or change their screen name if necessary. Children should never use their real name in a chatroom and should report any users who are breaking the rules set out by the chatroom provider.
- The best messaging apps will use encryption while transmitting the data, so that it can't be intercepted and read by others. Many have end-to-end encryption to protect messages along with other forms of communication, such as group chats, voice calls, media files etc.
- To ensure that there are no security flaws in any applications that children are using, make sure they are also kept up to date and install any patches as soon as they become available. Always check the terms and conditions of any applications that are being used, especially those around age. For example, by default, Skype restricts the privacy settings of users under 16 years old. However, this won't be effective if they are registered with parental information

- Help to educate your child on how to use these programs to ensure they are safe. Careless use of any technology can lead to a breach of personal security, downloading viruses or malware or even contact from people they don't know.
- Remind your child to never accept instant messages, phone calls, screen sharing or files from someone they don't know.
- Consider using a parental control tool like Skypito to manage who your children communicate with. Skypito requires parents to approve all of their child's Skype contacts, and allows them to restrict calls and chats with strangers.

TikTok

Like many other Social Media platforms, TikTok has an age restriction of 13 years old. Whilst TikTok can be very appealing to younger audiences, many parents and carers are reminding their children that they need to be 13 before having the app.

Some parents and children have reported inappropriate content on the app, others have raised concerns about the risks linked to the messaging function and children keeping profiles open in order to get more comments and shares.

In the Appendix is the link to a Panorama episode which looked into how safe TikTok really is.

Protecting your home network

It is important to make sure that your home network is secure. Increased use of the Internet for anything increases your risk of clicking on or downloading something nasty to your network, so it's important you have anti-virus / anti-malware software installed to ensure the safety of your family.

- Keep your anti-virus program updated daily and allow it to stay current. There are new attacks every day and the amount of malicious content on web applications is rapidly increasing in both frequency and expertise so it's important to stay up to date.
- If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it. It is best to set up your network so that only people with a wireless 'key' (i.e. password) can connect to your network.
- If your network is secure, users will be prompted for a password when they try to access it for the first time and there should be a padlock symbol next to the network name. If this doesn't happen, your network isn't protected and anyone will be able to join.
- It is always best to change the name of your network from that which was originally provided – but not to anything that identifies it to you or your family. You should also change the default password, as these are often freely available to attackers online if they know where to look. You should choose a password of at least 8 characters, with a mix of case, numbers and symbols. The current advice is to pick three random words or a memorable phrase.
- Always cross-check information if you're not sure about what your child is being asked to do and speak to the school contact.

9. Reporting concerns

It is essential to have clear reporting routes so that children, teachers, parents and carers can raise any safeguarding concerns in relation to remote online education.

The school's safeguarding procedures continue in line with our Child Protection Policy.

The Designated Safeguarding Lead is: Debbie Christopher:
dchristopher@cirencesterkingshill.gloucs.sch.uk Tel: 01285 651511

The Deputy DSL is: Jeremy Morland: jmorland@cirencesterkingshill.gloucs.sch.uk Tel: 01285 651511

The school's approach ensures the DSL or a deputy is always contactable while the school is open. All staff will be re-issued with contact details for the DSL's during school closure and should report any concerns via email or telephone Mrs Christopher direct. *A member of SLT will be on site at all times while school closures are in operation.*

Staff will continue to follow the Child Protection procedure and advise the safeguarding leads immediately about concerns they have about any child, whether in school or not. COVID-19 means a need for increased vigilance due to the pressures on services, families and young people, rather than a reduction in our standards.

In addition to this, teachers, pupils, parents and carers can be referred to the practical support that's available for reporting harmful or upsetting content as well as bullying and online abuse, as outlined below and in the appendix.

Harmful or upsetting content

- reporting harmful online content to the [UK Safer Internet Centre](#)
- getting government advice and trusted resources from [Educate Against Hate](#) on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Bullying or abuse online

- get advice on reporting online abuse from the National Crime Agency's [Child Exploitation and Online Protection command](#)
- get advice and support from [Anti-Bullying Alliance](#) for children who are being bullied

Personal data and GDPR

As a school, we continue to follow our GDPR policy to inform our approach to data protection. This is available on the school website at:

<https://www.cirencesterkingshill.gloucs.sch.uk/assets/Policies/2019/Data-Protection-Policy.pdf>:

In the event of any concerns or breaches of data protection, these should be reported to:

- Mr Darren Stillman, Data Protection Officer: dstillman@cirencesterkingshill.gloucs.sch.uk
- Mr Duncan Evans, Data Protection Manager: devans@cirencesterkingshill.gloucs.sch.uk

In the context of online learning, it is important to emphasise the following points:

- Personal information including specific pupil progress information will not be shared with others in online lessons/forums.
- We will seek consent for any use of pupils personal information, including photographs/videos for marketing or promotional services.

- Staff are asked to take care to not share contact details when emailing multiple people.
- Staff and pupils are asked to take care when sharing usernames and other personal data for access

Staff, Pupils and Parents/Carers are also advised that information we retain includes:

- Login activity, specifically, the last time a student logged in to their email, Microsoft Teams/Show My Homework account.
- Within Teams, the date and time of if/when a pupil views any assignments or/and when they submit any work that is set
- This is to assist us in making sure pupils are engaging in learning sufficiently and so that we can generate appropriate and relevant feedback to pupils/parents/carers.

Appendix: Safeguarding pupils and teachers online

Support for School Staff on e-safety in the context of remote learning:

- remote education advice from [The Key for School Leaders](#)
- advice from [NSPCC on](#) undertaking remote education safely
- guidance from the [UK Safer Internet Centre](#) on remote education
- Schools can access the free [Professionals Online Safety Helpline](#) which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.
- Guidance on [teaching online safety in schools](#) provides information to help schools ensure their pupils understand how to stay safe and behave online.

Support for Parents/Carers on e-safety in the context of remote learning:

- [support for parents and carers to keep children safe online](#), which outlines resources to help keep children safe from different risks online and where to go to find support and advice
- guidance on [staying safe online](#) which includes information on security and privacy settings
- [Thinkuknow](#) provides advice from the National Crime Agency (NCA) on staying safe online
- [Parent info](#) is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Internet matters](#) provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [London Grid for Learning](#) has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Net-aware](#) has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- [Let's Talk About It](#) has advice for parents and carers to keep children safe from online radicalisation
- [UK Safer Internet Centre](#) has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services
- <https://www.bbc.co.uk/iplayer/episode/m000p3p9/panorama-is-tiktok-safe> Footage from a Panorama documentary, reviewing the use of TikTok by teenagers.
- [Reporting to CEOP video \(thinkuknow.co.uk\)](#)
- [Internet matters](#) - for support for parents and carers to keep their children safe online
- [South West Grid for Learning](#) - for support for parents and carers to keep their children safe online

Written by Jeremy Morland, 22 Jan 2021

This policy has been remotely approved by: Curriculum and Pastoral Governors, Andy Johnson and Maureen Richards on 22nd January 2021