This Addendum must be read in conjunction with the School's own Online Safety Policy, brought to the attention of those currently employed or volunteering in the school and shared with those individuals upon induction to the setting. It should be available to parents and displayed on the school website.

ONLINE SAFETY POLICY & PROCEDURES – COVID-19 ADDENDUM

September 2020

Approved by[1]	
Name:	Richard O'Connor
Position:	Assistant Head Teacher
Signed:	*R. O'Connor*
Date:	15/10/2020
Proposed review date[2]**:**	October 2021

REVIEW SHEET

The information in the table below provides details of the earlier versions of this document and brief details of reviews and, where appropriate amendments which have been made to later versions.

Version Number	Version Description	Date of Revision
1	Original	September 2020

CONTENTS

1 Introduction

This addendum has been created following DfE guidance Actions for schools during the coronavirus outbreak (Full Opening: Schools), Actions for Early years and childcare providers and Actions for Special schools and other specialist settings and applies to all schools (mainstream and alternative provision): primary, secondary (including sixth forms), infant, junior, middle, upper, school-based nurseries and boarding schools. Independent schools are expected to follow the same control measures in the same way as state-funded schools. It is an addendum to the School's Online Safety Policy and procedures and must be read in conjunction with the Online Safety Policy, Whole School Behaviour Policy and (for staff and other adults) the Code of Conduct for Staff and Other Adults (including the Addendum to these). The school's Online Safety Policy along with this Addendum must be available on request and must be read and understood by all those individuals involved in providing remote education children and young people in the school.

All staff have a responsibility to be aware of systems within their school which support safeguarding and any temporary amendment to these will be explained to them by senior managers. This includes the school's Child Protection Policy and procedures, the school Code of Conduct or Staff Behaviour Policy, the Online Safety Policy and the associated Acceptable Use Agreements.

2 Context

From 20 March 2020 parents were asked to keep their children at home, wherever possible, and for schools to remain open only for those children of workers critical to the Covid-19 response - who absolutely need to attend.

From 01 June 2020, schools were asked to open to more pupils in addition to the children of key workers and those who are deemed vulnerable.

From the beginning of the autumn 2020 term, all pupils, in all year groups, should return to school full-time.

Despite the changes, **our Online Safety Policy is fundamentally the same** with this addendum setting out some of the adjustments we are making in line with the altered arrangements and following advice from government and local agencies.

This Addendum will be reviewed regularly as the nature of the pandemic and local or national responses that involve remote education, or government guidance on how we should operate significantly changes.

Some settings will have additional responsibilities arising from their regulation e.g. EYFS settings, or Special Schools as a result of their responsibility for young people over the age of 18.

Once adopted, this Addendum may be referred to in any disciplinary proceedings following unacceptable action by staff or other adults.

3 Online Safety and Remote Education

Although we aim to have all pupils back at school in the autumn, also need to plan for those who might need to self-isolate, the possibility of a local or national lockdown and how we will ensure continuity of education. During periods of lockdown in a pandemic, whether experienced by the whole community if Public Health advises us to close, or by individuals who become ill or receive a positive test result for Covid-19 or must self-isolate because they have come into close contact with someone who has, learning will move substantially online for most pupils.

Our Policies, procedures and supporting documents like our Acceptable Use Agreements have been reviewed to ensure they reflect how we will manage remote education and that they remain appropriate and useful for keeping people safe online during a pandemic.

- For individuals or groups of self-isolating pupils, remote education plans will be in place. These should meet the same expectations as those for any pupils who cannot yet attend school at all due to Covid-19.

- A local lockdown may involve a return to remaining open only for vulnerable children and the children of critical workers and providing remote education for all other pupils – plans will be developed to ensure these can be staffed and managed.
- Where a class, group or small number of pupils need to self-isolate, or there is a local lockdown requiring pupils to remain at home, we will ensure we have the capacity to offer **immediate** remote education.
- Our Emergency/Contingency Plan(s) will be reviewed/updated to reflect our plans should there be a spike in infections and schools are advised to temporarily close (local lockdown) - Refer to Local lockdowns: guidance for education and childcare settings. This will enable us to:
  - use a curriculum sequence that allows access to high-quality online and offline resources and teaching videos, and that is linked to the school's curriculum expectations;
  - give access to high quality remote education resources;
  - select the online tools that will be consistently used across the school in order to allow interaction, assessment and feedback, and make sure staff are trained in their use;
  - provide printed resources, such as textbooks and workbooks, for pupils who do not have suitable online access;
  - recognise that younger pupils and some pupils with SEND may not be able to access remote education without adult support, and so schools should work with families to deliver a broad and ambitious curriculum.
- When teaching pupils remotely, we will:
  - set assignments so that pupils have meaningful and ambitious work each day in a number of different subjects;
  - teach a planned and well-sequenced curriculum so that knowledge and skills are built incrementally, with a good level of clarity about what is intended to be taught and practised in each subject;
  - provide frequent, clear explanations of new content, delivered by a teacher in the school or through high quality curriculum resources and/or videos;
  - gauge how well pupils are progressing through the curriculum, using questions and other suitable tasks and set a clear expectation on how regularly teachers will check work;
  - enable teachers to adjust the pace or difficulty of what is being taught in response to questions or assessments, including, where necessary, revising material or simplifying explanations to ensure pupils' understanding;
  - plan a programme that is of equivalent length to the core teaching pupils would receive in school, ideally including daily contact with teachers.
- We will consider the above in relation to the pupils' age, stage of development and/or special educational needs, e.g. where this would place significant demands on parent's help or support. We will avoid an over-reliance on long-term projects or internet research activities.

To identify new or higher risks associated with remote education, people whose risks have changed, and ways risks can be reduced, knowledge of our school was used with information and advice published by the government, our Local Authority and a range of respected regional or national bodies who consult with the UK Council for Internet Safety regarding online safety like the Safer Internet UK partners and the NSPCC.

The main issues to address are:

- Equality of access to delivering and receiving remote education (looking at infrastructure, devices, and technical knowledge in homes and how any SEND or home circumstances might affect access); and
- The safeguarding of staff, pupils and others affected by remote education (looking at safe use of technology, safe teaching/learning environments, and safe behaviour especially regarding privacy and security).

3.1 Equality of access to remote education

When we participated in the DfE Laptops for Disadvantaged Children Programme, we took reasonable steps to support as healthy and secure a workstation set-up at home as circumstances allowed.

Before distributing devices, we will ensure:

- They are set up to access remote education.
- Appropriate safeguarding controls and support are in place to help children and families use devices safely.
- Help and support with technology is available to us to do all this successfully through DfE guides Get help with devices and Get help with technology, and the EdTech Demonstrator Programme, which provides access to a network of schools and colleges who are already using remote education technology resources.

Information is or will be made available to parents and carers who need it about:

- How we run our device loan scheme with devices from the DfE Programme, who owns the devices, responsibilities of borrowers, how we deal with loss, theft or damage, and repair or replacement arrangements for faulty devices under warranty.
- Connectivity support available for disadvantaged children through free BT wifi hotspots and increased mobile data allowances.
- Support for children with special educational needs and disabilities available from the Family Fund and/or the 16 to 19 Bursary Fund which 16 to 19-year-olds from disadvantaged households may be eligible for support from.
- DfE online education resources for home learning, and other online activities and resources to support remote education.
- DfE Coronavirus (COVID-19): support for parents and carers to keep children safe online when setting up and using technology for remote learning.
- Video Conferencing for Kids: Safeguarding and Privacy.

During periods of remote education we will rely on teaching resources recommended by the government, professional associations and other specialists in education. We will also follow government examples of remote teaching practice and guidelines on their use i.e. that they do not replace our properly planned curriculum.

3.2 Safeguarding during remote education

We recognise the additional risks to pupils associated with being online more than before the pandemic helpfully summarised by the South West Grid for Learning (SWGfL) report.

We also recognise additional risks for staff, especially those facilitating remote learning via video links that may impact other people in their household or community as well. As set out in the Coronavirus (COVID-19): safeguarding in schools, colleges and other providers guidance, online education should follow the same principles set out in our staff code of conduct which has been updated to reflect expected good remote education practice.

We will follow relevant government safeguarding guidelines and make use of recommended technical tools and guides to help us deliver remote education safely from organisations like The Key for School Leaders, and education and child protection specialists like SWGfL, London GfL and the NSPCC.

In addition to the updated codes of conduct, staff, pupils (or due to their age and ability, the adults supporting them), parents, carers, and to some degree, virtual or in-person visitors using online technology for education purposes or school business are expected to (with examples of support):

3.2.1 Check security and privacy settings

- Adjust privacy and safety settings on all devices, in apps and other online places to control what personal data is shared.

- Review the security settings on 'smart' devices and change any default, weak or guessable passwords.;
- Set up two-factor authentication if devices are capable or available. This is a free security feature to stop unwanted people getting into accounts. Users receive a text or code when they log in to check they are who they say they are.
- Regularly update devices or apps used for school or work. Using the latest version of software and apps can immediately improve security.
- Think about physical privacy when appearing live online e.g. the appropriate adult supervision of children at home, appropriate clothing, distractions like noise and interruptions, what other people nearby can hear.

3.2.2 Act regarding unsuitable content

- Prevent unwanted content from appearing i.e. set filters and parental controls on home broadband and mobile networks and not disable or bypass them (the UK Safer Internet Centre has advice on how).
- Block unsuitable contact (with support as necessary)
- Report harmful activity, to the website, platform or app, a trusted adult and the Designated Safeguarding Lead. Report Harmful Content to Safer Internet UK if not satisfied with the result of a report to a service provider.

3.2.3 Protect against fraud

- Beware of fraud and scams online including Covid-19 related phishing emails and text messages and use appropriate cyber security and "stop, challenge, protect" information to avoid becoming a victim.
- Forward suspicious emails to report@phishing.gov.uk, a service run by the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service to get them removed automatically if they fail NCSC validity tests.
- Never give out personal information to websites or in response to emails/text messages not recognised or trusted
- Report being scammed, defrauded or experiencing cyber-crime to Action Fraud, the UK's national reporting centre.

3.2.4 Check the Facts

Use the SHARE checklist to make sure they are not contributing to the spread of harmful content e.g.

- **S**ource - make sure information comes from a trusted source
- **H**eadline - always read beyond the headline (use the NewsGuard free tool to help identify fake news).
- **A**nalyse - check the facts (use the Ofcom Cutting Through the COVID-19 Confusion webpages, check claims about COVID-19 at Full Fact and find reliable information from www.gov.uk/coronavirus).
- **R**etouched - does the image or video look as though it has been doctored?
- **E**rror - look out for bad grammar and spelling

3.2.5 Stay physically and mentally healthy online

Whether staff or pupils are working, learning or playing online, they should take regular breaks and use tools like Apple's Screen Time, Google's Family link, Xbox One, Playstation 4, Nintendo Switch if necessary to manage screen time, especially:

- if they're feeling overwhelmed, perhaps limiting the time spent watching, reading, or listening to coverage of the outbreak, checking in at set or just a few times a day
- if they're feeling physical discomfort like aches, pins and needles, pain, strain, headaches; or
- if they need to be more physically active outdoors.

Parents and carers will be given guidance on supporting their child's mental health and wellbeing during COVID-19 as well as screen time advice from the Chief Medical Officer. We will also provide practical guidance on making the home environment a good and safe one to learn in with a sensitive appreciation for people's different home circumstances and what is reasonable.

Staff are also expected to:

- Provide information about their temporary home working environment insofar as it might impact on their physical health, or the safeguarding of learners or their own household.
- Act appropriately on feedback and use any necessary online or cyber tools provided.
- Provide information about the technology they use at home to get online i.e. to ensure compatibility with school systems, especially cyber security measures involved in accessing sensitive data like medical, behaviour or performance information on school servers remotely.
- Implement relevant guidance on safe teaching and pastoral care from their home e.g. what is in the background of recorded or live streams, what is visible on shared screens, what can be heard by others in a household etc.
- Pay special attention to how they protect personal data at home.

3.2.6 Keep talking about staying safe online

Which we can do by:

- Ensuring staff have the tools to promote a healthy balance between the positive and negative aspects of life online.
- Signposting parents and carers to tools to explain and reduce risks, and help them talk to their child (e.g. UKCIS guidance on minimising children's exposure to risks; Childnet International's conversation starters and specific guidance on under 5s; Ditch the Label teacher resources that can be helpful for parents to discuss cyberbullying; the government's helpful advice; and where there are concerns about specific serious harms, the guidance on how to protect your child from child sexual abuse online, 'sexting' or radicalising, pornographic or suicide content).
- Reiterating behaviour expectations and ways to handle and report problems, especially encouraging children to speak to a trusted adult if they come across content online that makes them uncomfortable.
- Supporting critical thinking and promoting resources like Parent Zone's guide and Childnet's advice and top tips which provide ways parents and carers can help their child develop these skills.