ZENITH
MULTI ACADEMY
TRUST

Safe Remote Teaching/Learning/ Working Policy

for use in:
All schools in the Trust (including Castledon's Satellite)
Central Team
Zenith Minds
LocalGoverningBodies/LocalAdvisoryGroups
Trustees
Governors
Members

Approved by:	Standards Committee
Date:	June 2026
Last reviewed:	July 2025
Next review due by:	June 2027 (Or sooner if guidance changes)

Contents

1.	Introduction and aims	1
2.	Relevant legislation and guidance	1
3.	Roles and responsibilities	1
4.	Remote teaching systems	2
5.	Student expectations	2
6.	Staff expectations	3
7.	Further considerations	4

1. Introduction and aims

It is crucial to ensure school staff and students are able to engage safely and effectively in remote teaching, learning and working arrangements during periods where education cannot take place fully on site. This policy supports the trust's Acceptable Use Policy and Child Protection Policy, and other relevant policies governing the safe use of technology away from school.

This policy applies during emergency or unplanned school closures, including but not limited to severe weather events, public health incidents, utility failures, site emergencies, or other circumstances that prevent normal school operations.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, students, parents and governors whilst working from a remote location
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety, and safeguarding
- Support the school in teaching students safe and effective internet and ICT use

Breaches of this policy will be dealt with in line with our behaviour policy and staff discipline/staff code of conduct policies

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools
- Safeguarding and Remote Education 2022
- Emergency planning and response for education, childcare, and children's social care settings

3. Roles and Responsibilities

The following individuals are either directly involved or are mentioned throughout this policy.

School	Name	Role
Zenith Multi Academy Trust	Lauren Goodwin	Trust Safeguarding Coordinator
Zenith Multi Academy Trust	Sean Goodwin	Director of ICT Services
Zenith Multi Academy Trust	Alan Mechem	Director of Marketing and Communication
The King John School	Keith Green	Designated Safeguarding Lead

James Hornsby School	Dee Sumner	Designated Safeguarding Lead
Castle View School	Lizzie Hobbs	Designated Safeguarding Lead
Laindon Park Primary School	Cristina Portoles	Designated Safeguarding Lead
Castledon School	Jon Hazelgrove	Designated Safeguarding Lead

4. Remote Teaching Systems

Each school within the trust has independent systems in place to provide remote learning. These are:

The King John School:	Microsoft Teams King John Student Portal
Castle View School:	Microsoft Teams,
James Hornsby School:	Google Classroom, TES Class Charts
Laindon Park Primary School:	Microsoft Teams
Castledon School:	Google Classroom

Trust schools will ensure they are able to offer a remote education provision during emergency or unplanned school closures.

Schools will communicate arrangements for remote learning, including lesson delivery, attendance expectations, methods of submitting work and how students can seek support during periods of remote education.

To support this provision staff may utilise one of the school's pre-approved platforms to deliver a live video-based lesson. Students and staff must follow the expectations outlined in point 5 and 6 when participating in the remote delivery of a lesson.

5. Student Expectations

- Students must ensure they only communicate with members of staff through authorised channels, such as their school email accounts and learning platforms .
- If students have been advised to sign up for online systems for use with subjects, ensure a school provided email address is used (not a personal one) and have a strong, secure password.
- Students must download and install any updates for their laptop/computer to ensure they have the latest security patches.
- Students must only post about schoolwork in the 'Stream' (Google Classroom) or 'Posts' (Microsoft Teams) section if this has been enabled by the teacher. Inappropriate posting or bullying will be sanctioned in line with the school's behaviour policy.
- Students must not copy or download images/ pre-recorded videos uploaded by Teachers to Google Classroom/ Microsoft Teams.
- Students must not use Google Classroom/ Microsoft Teams to send private messages/call members of staff
- Students must ensure that they only participate in live lessons that have been pre-arranged by the school. Do not join online classes that you have not been instructed to join by a teacher.
- Students must not record or photograph live lessons unless given direct written permission from the member of staff providing the lesson.
- Students must ensure they follow the same expectations outlined in the school's behaviour policy when working remotely. Sanctions can and will be applied as necessary should conduct

fall below what is expected of our students. Students will receive reminders around the conduct that is expected of them in these circumstances.

6. Staff Expectations

- Staff must only access personal data of other staff members and students through their school's remote access provision.
- Documents including personal data about other staff members and students must not be downloaded and stored on personal devices.
- Staff must not share devices used for accessing school systems with unauthorised individuals.
- Staff must not write passwords to ICT systems and accounts on physical documents that may be viewed by other individuals.
- Printed documents including official-sensitive information must not be left unattended and should be stored out of access from other individuals.
- Staff must ensure they lock devices when not using them to prevent sensitive information from being viewed by other individuals.
- Staff must ensure that any devices they are using have reliable antivirus and anti-malware software. School provided devices will already have this installed.
- Staff should remain alert to common cyber threats such as phishing emails, malicious links, or unauthorised access attempts. Any concerns must be reported immediately to the IT Support team.
- Staff must ensure multifactor authentication (MFA) is enabled on remote platforms where possible.
- Staff must download and install any updates for your laptop/computer to ensure they have the latest security patches.
- Staff must only use school provided email accounts, learning platforms or EduLink One to communicate with students and parents.
- Staff must ensure that any resources uploaded to support students learning do not include any personal information that could identify other pupils, such as names or comments addressed specifically to them.
- Staff recording videos to be shared via school social media/ YouTube accounts must be recorded against a neutral background, ensuring they are dressed appropriately for a school environment. Any videos that staff wish to make available to students must contact the trust's Director of Marketing & Communication.
- Staff required to phone parents should do so using a school authorised telephone within school hours, not through personal devices. Ensure a record is kept of dates and times.
- Staff required to phone pupils ensure they do so with a school authorised telephone and only to the parent's phone. Ensure the student has a parent present and ask the student to have the phone on speaker phone. Ensure you take a written record of the conversation.
- Staff providing live lessons should do so using only the provisions outlined by their school (Microsoft Teams/ Google Classroom). Staff must also consider implications for those who do not have access and those with special educational needs.
- Staff should ensure resources and lesson content are accessible for students with additional needs, including those with EHCPs. This may include the use of captioned videos, screen-reader-friendly materials, simplified formats, or alternative tasks in consultation with the SENCO.
- Staff should ensure live streams are broadcasted from a suitable location, ensuring they follow the guidance above for recording videos. Ensure students participating in a broadcast live lesson have their web cam turned off.
- Staff must be aware of the school's procedures for filtering and monitoring, as set out in their annual safeguarding training, staff Code of Conduct, and Online Safety Policy.
- Staff should continue to act immediately if they have any concerns about a child or young person's welfare, whether the child or young person is physically in school or learning from

home. Staff working remotely should continue to raise concerns and follow the safeguarding procedures outlined in the school's Child Protection and Safeguarding Policy.

7. Further considerations

Schools must continue to provide a safe environment, including where learning is delivered online. Schools should continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the school's IT systems or recommended resources.

Schools must make reasonable adjustments to ensure students who lack access to devices or stable internet can still engage with learning. This may involve the loaning of devices, distribution of printed materials, or flexible deadlines. Schools should monitor and log students' access needs and provision regularly.

All schools should be doing what they reasonably can to keep their children safe. It is important that all staff who interact with children, including online, continue to look out for signs that a child may be at risk. Any such concerns should be dealt with as per the child protection policy and where appropriate referrals should be made to appropriate external agencies.

The Zenith Multi Academy Trust is following DfE guidance on providing education remotely. The schools network managers and the MAT Director of ICT Services need to ensure they are up to date with this guidance. All schools must consider the safety of their children when they are asked to work online. The starting point for online teaching should be the same principles as set out in the school's staff code of conduct. Schools must ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online.

As well as reporting routes back to the school this should also signpost children to age appropriate practical support from the likes of:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

It is important that parents/carers are aware of what their children are being asked to do online, including sites they will asked to access and be clear who from the school their child is going to be interacting with online. Parents/ carers may choose to supplement support from online companies and in some cases individual tutors. Schools should emphasise the importance of securing online support from a reputable organisation/individuals. The following resources are recommended, as linked in Keeping Children Safe in Education 2024:

- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world
- How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online
- London Grid for Learning provide support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP/ Thinkuknow provide support for parents and carers to keep their children safe online
- Parentzone provides help for parents and carers on how to keep their children safe online
- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment