WYNDHAM
SPENCER ACADEMY

E-Safety Policy

September 2021

The Spencer Academies Trust has delegated Full responsibility to the Local Governing Body (LGB) of Wyndham Spencer Academy for this Policy.

It is the LGB's responsibility to ensure this Policy is implemented and reviewed in accordance with statutory and legislative arrangements.

The Spencer Academies Trust may, on an annual, basis undertake audits to confirm that appropriate arrangements are maintained by the Academy.

SPENCER
ACADEMIES TRUST

Introduction

This policy aims to cover the different elements of safeguarding and promoting our pupils' safe use of internet and electronic communication technology. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

This policy will operate in conjunction with others including: policies for Safeguarding, Behaviour, Anti-Bullying, Equality and Acceptable Use Agreements with staff, pupils and parents. The e-safeguarding policy works in line with the GDPR data guidelines and regulations from 2016/679.

Wyndham Spencer Academy recognises e-safety as an important issue for our school community and has made a considered attempt to embed e-safeguarding into our teaching and learning using technology and have considered the wider implications of e-safety beyond classroom practice such as security and data.

Effective E-safety practice.

E-Safety depends on effective practise in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-safety policy;
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used, including those associated with the PREVENT duty.

Aims and objectives

- To set out the key principles expected of all members of the school community with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Wyndham Spencer Academy
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of Policy

This policy applies to the whole of Wyndham Spencer Academy's school community: Senior Leadership Team, school board of Governors, all staff employed directly or indirectly by the school, volunteers and all pupils.

The Senior Leadership Team and school board of Governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers Principals, 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-Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will clearly detail its management of incidents within this policy and the anti-bullying policy and will, where known, inform parents and carers of incidents of inappropriate e-Safeguarding behaviour that takes place out of school.

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

Roles and Responsibilities - Senior Leadership Team

The Principal, Curriculum Directors and computing co-ordinator are responsible for monitoring the teaching of computing throughout the school. They will also oversee the completion of the computing concepts in each year group.

Roles and Responsibilities – Technology Leader

The computing coordinator will oversee planning in all year groups throughout the school and be responsible for raising standards in computing. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The computing coordinator is responsible for overseeing the assessment of computing across the school and providing opportunities to moderate computing ability.

Roles and Responsibilities – Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach computing and to use computing within their class. This will be in accordance to the schemes of work provided by the computing coordinator. They will also assist in the monitoring and recording of pupil progress in computing. Teachers should also respond to, and report, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as listed below. Staff should follow, and agree to, the Acceptable Usage Policy.

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and computing can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using computing and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through letters, Class Dojo, texts and parents' events.

Roles and Responsibilities – Pupils

Pupils should follow the school internet use guidelines. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities – Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the computing coordinator or the Principal.

Internet

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended.

The teaching of email and internet use will be covered within the computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of staff will be issued with a school email address and this is the email with which they should use for professional communication. Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the computing coordinator so it is the user's responsibility to ensure they log off appropriately.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to their class teacher who will subsequently report it to the ICT support team.

The internet and filtering is provided by the local authority and the ICT support team will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by AIT (Advanced IT Services)

Passwords

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

For online services used in school, such as blogs and Twitter, there is an account per class or year. For sites where children have passwords, e.g. Purple Mash, they will be provided with these by the computing coordinator. As children progress through the school they will be taught about having sensible passwords.

Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place.
Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents. (unless granted permission from the Principal).

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
When learning about emails, pupils will use Purple Mash 2 email.

- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- All confidential documents send between staff via email will be password protected.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations or parents, are advised to carbon copy (cc) or include the Principal, line manager or another suitable member of staff into the email.

Social Media

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.

- Not accept current or ex-pupils or parents as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community (such as children's parents) and ask that these members of staff take extra precaution when posting online.

- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children
- Check with the computing coordinator if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.
As a school we will use Twitter to post information, updates and blog posts. These will stream directly to our school website. We will ensure that we block any followers that appear inappropriate.

Digital and Video Images

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the computing coordinator. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online

Staff should not use personal cameras or phones to take photographs of children within school but instead use school iPads.

E-Safety Learning and Teaching

At Wyndham Spencer Academy we take E-safety very seriously. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.
We will ensure that it is taught regularly throughout computing, P4C and STREAM lessons. We will also provide children with dedicated e-safety lessons, where appropriate, by the Digital Leaders (see appendix 2). Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them. Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.

Pupils will be aware of the Acceptable Usage Policy (AUP) and will follow it at all times. All staff will also complete an AUP. Useful computing rules will also be posted in the computing suite an on the netbook trolleys to ensure they are seen by children and visitors. E-safety training will also be provided for staff and governors to ensure that they conduct themselves in the appropriate manner when working and communicating online.

If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the computing coordinator and Principal and recorded as appropriate.

Technical Support

Many minor issues are dealt with by the computing coordinator.
Additional hardware support is provided as and when necessary by George Spencer Academy.
Support for the website is provided by George Spencer Academy.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the computing coordinator who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the Principal. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Copyright and Intellectual Property Rights (IPR)

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet, will have discussions about the proper use of images, and should start referencing the sites they have used. This could be as simple as putting the name of the site the image came from or a hyperlink.

It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

Remote Learning

'Remote Learning' refers to the provision of work, teacher support, assessment and feedback from teachers to pupils in the event that normal lessons are unable to be delivered 'face-to-face' as normal.
Wyndham Spencer Academy is committed to providing continuity of education for its students in the event of an extended school closure. While such situations are inevitably highly varied in their causes and ramifications, we will endeavour to provide continued learning for our students during any period of closure in the following ways:

- Lessons provided on our dedicated year group YouTube channels
- Guidance of daily tasks on Class Dojo
- Regular Zoom calls as a class
- School will risk assess the use of live learning using webcams
- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- The live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- Leaders will reassure themselves that any teaching/learning software and/or platforms are suitable and raise no privacy issues; or use cases against the providers terms and conditions (for example, no business use of consumer products)

Parents are advised to follow the government guidance for online safety:
https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online

Training

Staff will be given biannual training as a minimum, with regular reference made to e-safety as part of the Safeguarding Hot Topics.
Parent workshops focussing on e-safety will take place during e-safety week with further guidance in the Safeguarding newsletters.

Appendix 1

Acceptable Usage Forms

Acceptable Usage Policy Key Stage 2 Children

When we talk about computing, we are talking about computers, iPads and everything else including cameras and other devices. By using the computing equipment in school, you have agreed to follow these rules.

☺ At all times, I will think before I click (especially when deleting files)

☺When using the internet, I will think about the websites I am accessing

☺When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site

☺ When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people

☺ When communicating online, I will only use my first name and not share personal details such as my email address or phone number

☺I know that the teachers can, and will, check the files and websites I have used

☺I will take care when using the computers and transporting equipment around

☺ I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers

☹ If I find a website or image that is inappropriate, I will tell my teacher straight away

☹ I understand that if I am acting inappropriately then my parents may be informed

☹ I understand that people online might not be who they say they are

☹ I will not logon using another person's account without their permission

Signed:

Acceptable Usage Policy Key Stage 1 Children

The Golden Rule: Think before you click

☺ I will be careful when going on the internet.

☺ I will only use the internet when a teacher is with me.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will keep my password secret, but I can tell my family.

☺ I will remember to log off properly before closing the lid of the chrome book.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't logon using someone else's username.

☹ I won't put water bottles on the table when using computing equipment.

Signed:

Acceptable Usage Policy

This document has been written to ensure that staff use the computing throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Management team or the computing Coordinator.

Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that they have a sensible password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer – particularly in shared areas
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's computing for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the computing Policy
- Be aware that software or hardware should not be installed without prior consent of the computing coordinator or Principal
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Principal
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Report any issues to the Senior Management team or computing Coordinator as soon as possible
- Return any hardware or equipment if they are no longer employed by the school

Signed _____ Print _____

Date _____

Acceptable Usage Policy Governors and Visitors

Visitors, both physical and virtual, may be provided with accounts to our network and/or online systems. Visitors will have a lower level of access than staff and each account will be provided on a case-by-case basis. This will depend on the purpose of the account requested.

Online Systems (Purple Mash, Google Apps, school website)

Visitors must provide the computing Coordinator with their name and email.
Users will:

- Not have access to mail or direct contact with children
- Understand that this account may be removed at any time so should not use it to save vital information

School Network and wireless

Users will:

- Be given a login for their time in the school
- Be expected to follow the guidelines as set out for staff
- Understand that this account may be removed at any time
- Be provided with the wireless key and guidelines for connecting to the network

Appendix 2

WONDER Curriculum

Digital Literacy E-safety			
Title	Passwords	Risks of online use	Fake information
Year 1	Understand why we use passwords	Understand that spending a long time in front of a computer screen can be unhealthy	
Year 2	Can remember a simple password and know not to tell anyone	Understand what makes a good online friend and the need to be kind and thoughtful online as in the real world	Know that not all information found online is true
Year 3	Understand the benefits of a good password	Understand that games and films have age ratings, and what that means Are aware that some people lie about who they are online	
Year 4	Can create and use a strong password	Can rate a game or film they have made and explain their rating	Recognise what kind of websites are trustworthy sources of information
Year 5	Understand what makes a strong password and why this is important at school and in the wider world	Recognise the benefits and risks of different apps and websites	Critically evaluate websites for reliability of information and authenticity
Year 6			Become increasingly savvy online consumers: know that algorithms are used to track online activities with a view to targeting advertising and information

Digital Literacy E-safety			
Title	Digital content	Personal information	Acceptable use
Year 1	Understand that you can share digital content online		Recognise inappropriate content and know to tell an appropriate adult
Year 2	Understand that digital content belongs to the person who first created it	Understand what personal information is and the need to keep it private	Know who to tell if concerned about content or contact online
Year 3	Understand that when we share content online, we might not be able to delete it	Understand when to share personal information and when not to	Know different ways of reporting unacceptable content and contact online
Year 4	Understand that the digital content we make belongs to us and that people can give permission for others to use their content e.g. using Creative Commons.		Demonstrate responsible use of online services and technologies, and know a range of ways to report concerns
Year 5			
Year 6	Know where to find copyright free images and audio, and why this is important		

Appendix 3

The impact of COVID-19 on the world has highlighted the importance of remote working.
At Wyndham Spencer Academy we have used various forms of remote learning to engage with students during this period of uncertainty.

- School will risk assess the use of live learning using webcams
- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- The live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- Leaders will reassure themselves that any teaching/learning software and/or platforms are suitable and raise no privacy issues; or use cases against the providers terms and conditions (for example, no business use of consumer products)

Parents are advised the following:

· Zoom is for children as a tool for learning, no guests or other grown-ups please (only the parent supporting their child)
· Do not share our links for learning or passwords with anyone
· Do not record the sessions or upload images from zoom to other platforms (including Facebook)
· Always use respectful language and remind anyone else who is in earshot to do the same
· Report any inappropriate language of individuals to the class teacher
· Stay in the Waiting Room until the class teacher checks everyone is a member of our school
· Please use your child's first name on each Zoom session (rather than a phone name)
· Ensure your child is fully dressed during the zoom meeting
· Consider what can be seen in the background during your meeting

Zoom Online Platform: risk assessment - Wyndham Spencer Academy

Initial Assessment conducted by: **Michelle Garton** **Reviewed and finalised by Kirsty Ryan**	Job title: **Vice Principal** **Principal**	Covered by this assessment: **pupils, staff, parents** and **other relevant individuals**.
Date of initial assessment: **15.6.20**	**[Updated]** Review interval:	Date of next review: **TBC in line with government updates**

Related documents
Annex to Child Protection and Safeguarding Policy: COVID-19 changes. March 2020

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major**	High (H)	H	Medium (M)
	Severe	H	M	Low (L)
	Minor	M	L	L

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
Link to Zoom session leaked beyond pupils/parents within the designated class	**M**	• Parents have to opt-in to zoom sessions each week through Dojo and link only shared with those parents • Link, room number and password only shared with parents in the class who have opted-in through a private message on Class Dojo • Staff to take a register prior to admitting pupils into the room to check they are pupils who have registered for the session. • Staff to set up Zoom accounts using their professional email address • Parents/children sent a zoom protocol reminder each week regarding expectations and privacy as follows: Hello, we're so pleased that you will be joining the Year X Zoom call t oday! The call will take place at X. We will be taking part in X Please see the details below for our meeting. You do not need an acc ount, you just need to click 'Join Meeting' and then login in using the meeting code and password. Here are the details to join: Topic: X Time: Jun 18, 2020 01:00 PM London Join Zoom Meeting (Link)	**Y**	**SLT & class teachers**		**L**

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		Meeting ID: 756 8724 5372 Password: 111111 Important details: - When you first enter the details, you will be placed in a 'waiting room.' Please stay in this room as we will be doing an electronic register before letting everyone in together. Following our Safeguarding Policy, the meeting will be 'locked' at X to ensure no one else can enter. - Make sure you use your real name during the session (first names only) so that we can safely admit all pupils we have on our register. Any pupils not on the register will not be admitted. - Upon entering, you will be muted. This is to try and control the noise and make sure we can all hear everyone. If you wish to add to the conversation, please put your hand up and you will be unmuted in turn. - To ensure we are following our Safeguarding Policy, it is vital to understand that you must not record this meeting in any way. That includes screenshots, photos or voice recording.				

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
Uninvited/unknown person gaining access to the meeting	**M**	• Staff member has the list of expected participants and they all wait in the waiting room prior to the session. • Staff member to admit pupils to the zoom session individually • Anyone not on the expected register will not be admitted • The room is locked 5 minutes after the session has begun	**Y**	**Class teachers**		**L**
Unauthorised recording of sessions	**M**	• No consent for data to be recorded – this will be switched off in account settings • All staff members are aware that recordings/photos are not allowed and raise this with parents each week prior to every session • Expectation of not recording is set out in the zoom expectations each week (above)	**Y**	**Class teachers & expectations monitored by PDs**	**Any incidents to be recorded on CPOMs immediately after the session**	**L**
Children not being supervised whilst taking part in the zoom session	**M**	• Parents to be aware of guidance and require consent before the session • Parents to be in the room during meeting to supervise their child	**Y**	**Class teachers**	**Any incidents to be recorded on CPOMs immediately after the session**	**L**

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
Inappropriate behaviour/contact	**M**	• Wyndham staff members to always be present during zoom sessions. Where possible, this will include 2 staff members • The host of the zoom session will always be a Wyndham staff member with DBS clearance and will have agreed to carry out protocols as set out in the safeguarding policy (including the Annex to Child Protection and Safeguarding Policy: COVID-19 changes) and Zoom Risk Assessment • Any additional 'visitors' who join a zoom session (e.g. a nurse during the lockdown heroes week or transition leads from secondary schools) will have read the Zoom Risk Assessment and agree to comply with the guidance through sending back a digital signature to Michelle Garton (mgarton@wyndhamacademy.org) prior to the session	**Y**	**Class teachers & Michelle Garton**	**RA to be signed and sent 1 week prior to the session with any 'visitors'** **Any incidents to be recorded on CPOMs immediately after the session**	**L**
Inappropriate sharing of personal information/contact details	**M**	• Expectations sent out weekly prior to each zoom session otherwise pupils will be removed from the room • Staff to ensure they are in a neutral space, without personal information visible • Parents to ensure they are in a neutral space, without personal information visible • Staff members to visually scan each pupils' background at the earliest opportunity to establish any inappropriate/sensitive background	**Y**	**Class teachers**	**Any incidents to be recorded on CPOMs immediately after the session**	**L**

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
Inappropriate clothing/setting for sessions	**M**	• Clear guidelines to all parents/pupils on wearing suitable clothing and suitable location for accessing meeting • Staff members to monitor clothing/locations. Anyone who is not following the expectations to be removed from the Zoom session, depending on level of inappropriateness or parents spoken to via phone call after the session.	**Y**	**Class teachers**	**Any incidents to be recorded on CPOMs immediately after the session**	**L**

I can confirm I have read the above risk assessment relating to the use of using Zoom as an online platform with pupils and staff from Wyndham Spencer Academy.

I confirm that I agree to adhere to the expectations as set out above.

Signed: Role: