Online Safety Policy

September 2023

This policy was agreed by the governing body on …….. and will be reviewed as required. Signed: Chair of Governors : Caroline Smith Date:

•

•

Statutory Policy

The aims of this policy are:

- To keep everyone safe online.
- To help develop a culture of openness about life online and how to stay safe.
- To guide staff, volunteers and governors in how to keep pupils safe online with regards to the curriculum and to internet filtering and monitoring.
- To comply with legislation regarding online safety.

Writing and reviewing the Online Safety Policy at Glen Hills Primary School:

- The Online Safety Policy relates to other policies including those for Curriculum, Teaching and Learning, Behaviour, Anti-Bullying, Safeguarding, Child on Child abuse and IT Acceptable Use documents (this list is not exhaustive).
- The Head teacher, leadership team, safeguarding team and Computing Leader have the overview for Online Safety in the school.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- This policy has been written following the most up to date guidance in Teaching Online Safety in Schools, DfE.

The 4 Cs of online safety:

An important step in improving online safety at your school is identifying what the potential risks might be.

Keeping Children Safe in Education 2023 groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the **4 Cs of online safety.**

1. **Content**

Content is anything posted online - it might be words, images and/or video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

2. **Contact**

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like child on child abuse (see policy on this, peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

-
-

3. **Conduct**

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

4. **Commerce**

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Glen Hills Primary School also considers how the risk from commerce applies to staff.

Roles and Responsibilities

The DSL/ Head teacher (and where appropriate, Computing Leader) will:

- Take day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents, in partnership with the school's DSL and DDSLs as required;
- Promote an awareness and commitment to online safety throughout the school community;
- Ensure that Online Safety education is embedded across the curriculum
- Liaise with school IT technical staff;
- Communicate regularly with the Governing body to discuss current issues, review incident logs and filtering / change control logs;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident;
- Ensure that staff are trained appropriately in online safety and reporting concerns
- Provide parents/carers with guidance about current online issues
- The DSL is responsible for ensuring the appropriate filtering and the monitoring of this is in place when pupils access the internet in school.

Teaching and learning

Importance of internet and digital communications

Being online is an essential element of life in the 21st century for education, business and social interaction. The school has a duty to deliver Online Safety content across the curriculum, which ensures pupils use the internet and technology in a safe, considered and respectful way, so that they can successfully and positively participate in the online world. Pupils will also explore where to go for help and support when they have concerns about content they encounter online.

•

•

Being online is a part of the curriculum and a necessary tool for staff and pupils. The benefits of being online in education include:

- Access educational resources to enhance and enrich the taught curriculum
  Support to scaffold learning across the curriculum
- Educational and cultural exchanges world-wide
- Cultural, vocational, social and leisure use in and beyond the school setting
- Engagement in research and expertise in various curriculum areas
- Staff continuous professional development to stay up to date with current educational initiatives and practices
- provide a platform for smarter working practices to reduce workload
- Access to a broad range of professionals to enhance the curriculum, pupil wellbeing and safety

Online Safety Curriculum

- The school will deliver an Online Safety curriculum that is regularly reviewed and updated.
- The Online Safety curriculum will reflect current statutory and non-statutory guidance and good practice.
- The school will ensure that Online Safety curriculum is progressive, age-related and scaffolded where necessary, to meet the needs of all pupils.
- Staff will reinforce Online Safety messages in the use of IT across the curriculum.
- Pupils will be taught what being online includes and acceptable practices.
- Pupils will be taught what is not acceptable online and be given clear objectives for online activity.
- Pupils will be educated in applying effective strategies to engaging positively in life online.
- Pupils will be shown how to publish, present and share information appropriately to a wider audience.
- Pupils will be taught how to navigate, manage and evaluate online content, through explicit coverage of Online Safety strands.
- Pupils will be taught to identify potential harms and risks online.
- Pupils will be taught to be critically aware of the materials they read and they will be shown how to validate information before accepting its accuracy.
- Pupils will be taught how and when to report unpleasant online content e.g. older pupils may be taught to use the CEOP Report Abuse icon. All pupils will be taught to report online concerns to a trusted adult without delay.
- Pupils will be taught to recognise techniques used online for persuasion.
- Pupils and staff will be taught / discuss how technology can affect wellbeing.
- Teachers will refer to relevant school documentation and the DfE's 'education for a connected world framework' and 'ProjectEvolv' to plan, deliver and resource Online Safety curriculum content.
- PSHCE curriculum for anti-bullying (including cyber bullying)

-
-
- Use of lessons and resources from https://projectevolve.co.uk/ for online safety content.
- Internet safety day Tue, 6 Feb 2024
- Y6 computing safety talk at SATS evening
- Relevant e-safety resources shared with home regularly.

Communicating and introducing the Online Safety Policy to pupils

- Appropriate elements of the Online Safety Policy will be shared with pupils.
- Pupils will be informed that network and online activity will be monitored.
- Curriculum opportunities to gain awareness of online issues and how best to deal with them will be provided for pupils.

Acceptable Use

Staff and Governors

- Use of school IT systems is governed by IT Acceptable Use Policies (see appendices), which ensure that all staff and pupils will be safe and responsible online users and of other digital technologies.

All staff will be expected to sign to say they have read the Online Safety Policy on an annual basis.

- All staff must read and sign the **IT Acceptable Use Policy for Staff and Volunteers** as part of their induction, before using any school IT resource. This can be found within the appendices of this policy.
- Any person not directly employed by the school will only be allowed supervised access to the school's IT systems (other than trainee teachers).
- All volunteers will sign an IT acceptable use policy on induction.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Failure of staff to comply with the IT Acceptable Use Policy may result in disciplinary action.
- Staff who manage filtering systems or monitor IT use will be supervised by senior leadership and have clear procedures for reporting issues.

Pupils

- All Pupils and parents/carers will be asked to sign and return the Pupil Acceptable Use Policy (see appendices). Information will be shared with new starters at the school in their information packs.
- Failure of pupils to comply with the Pupil Acceptable Use Policy will be dealt with in accordance with the school's Behaviour Policy.
- Cyber-bullying will be dealt with in accordance with the school's Anti-Bullying Policy.
- Pupils deemed as being 'vulnerable online' will be flagged to the Designated Safeguarding Lead, and tailored provision for using technology will be considered.

•

•

Community use of the internet

• All use of the school internet connection by community and other organisations shall be in accordance with the school Online Policy.

IT Systems

Information system security

- School IT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Symphony Learning Trust and reviewed regularly.

Filtering

- The overarching responsibility for filtering systems in school lies with the school's DSL.
- Staff, volunteers and governors understand their duty to keep children safe online using the school's internet.
- Staff and governors are trained annually at a minimum to understand their statutory duties regarding online filtering, e safety, how the school keeps children safe online through filtering and also how this is monitored.
- Volunteers are trained when they are inducted – appropriate information is included in the staff/induction handbook. Volunteers read, understand and sign the IT Acceptable Use policy for volunteers.
- Staff, volunteers and governors understand that the internet is continually changing, and that vigilance is key.
- School internet access is provided by Wave9 and includes filtering appropriate to the age of pupils.
- The school works in partnership with IT consultants to ensure systems to protect pupils are reviewed and improved.
- The school has levels of filtering in place (for example, a different level for staff including social media for marketing of the school and for teaching resources such as You Tube).
- The school will perform checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Monitoring of filtering

- If staff or pupils come across unsuitable online materials, it must be reported to the Designated Safeguarding Lead (DSL) (or a Deputy DSL in their absence), which is investigated immediately and the device removed.
- Should there be a breach, the breach is logged and investigated and actioned by the DSL and IT team.
- This log is reviewed regularly, to ensure actions to be taken are completed, by the safeguarding team.
- Should a pupil be found to be searching for inappropriate materials in school, parents/carers would be informed by the school, support and education offered to

-
-

  both parents/carers and the pupil, and a log be made on the child's CPOMS safeguarding record under the tag 'e-safety incident/concern'. (See flowchart of how to respond to an online incident in appendices).
- The IT team complete a regular filtering log check to report to the DSL and action anything suspicious or concerning with Senso (or other appropriate system). They action this to ensure that such materials can no longer be accessed.
- The school engages in regular external filtering testing using the KCSIE recommended SWGFL Test Filtering and obtains a certificate of evidence.
- Governors understand their statutory duty to monitor filtering. The safeguarding governor checks the school's logs and incidents reported where a child/staff member/volunteer has accessed or tried to access inappropriate information online. This will be reported to governors and as part of the annual safeguarding audit.

Accounts

- Staff will be provided with a local account for their device and a G Suite or google account with a linked e-mail address (ending in @glenhills.co.uk).
- Pupils will access the local network via a pupil/year group account.
- Guests will have access to a guest group account where needed.
- Pupils have LAN access via whole school shared drives and year shared drives when on certain devices. Pupils are monitored and supervised at all times when accessing these.
- Staff and pupils will be provided with additional accounts as determined by the school (e.g. to access online teaching and learning resources).
- Use of all school-related accounts will be in accordance with the IT Acceptable Use Policy.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system (those ending in @glenhills.co.uk or @symphonylearningtrust.co.uk).
- Pupil access to e-mail will be restricted and monitored at all times. Pupils will not be able to use their email addresses to send and receive emails, but for log in purposes only. Pupils can send and receive emails in line with the pupil IT Acceptable Use policy.
- Email accounts of pupils may be used on infrequent occasions by teachers and pupils in their class during the teaching of using emails safely. This will be closely supervised.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- School will delete email logins for pupils once they leave the school.

-
-

Videoconferencing (to be used alongside the school 'Remote Learning Procedure' documentation)

- If used, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call and be supervised at all times during a call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Social networking

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils must not place personal photos on any social network space without permission.
- Pupils, parents/carers and staff will be advised on the safe use of social network spaces (those appropriate for primary pupils).
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils and parents will be reminded about relevant age restrictions when discussing use of social media.
- The use of social media is not permitted at Glen Hills Primary School and pupils attempting to access this will be in breach of the IT Acceptable use policy.

Devices - including smart and mobile technology

- School-managed technology will be used by staff and pupils in accordance with the IT Acceptable Use Policy.
- All school devices will be managed carefully and pupils' use of them will be for solely educational purposes.
- Use of personal devices in school will be in accordance with the IT Acceptable Use Policy (for adults only- pupils do not have access to the internet freely in school).
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.
- Pupils are not permitted to have personal mobile phones switched on in school. Any child bringing a mobile phone to school for safety reasons (ie walking home independently), signs a Mobile Phone Policy (along with parents/carers), and switches the device off whilst on site. Phones handed in to staff upon arrival at school.
- Pupils are not permitted to wear smart watches in school.
- Pupils are not permitted to take smart/mobile technology on trips (including residentials).
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff should not share personal telephone numbers with pupils and parents/carers.

•

•

Managing emerging technologies

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Use of personal data and copyright

Published content and the school website

• The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The 'contact us' page directs emails to the office email address.

- The Head teacher will take overall editorial responsibility and ensure that content is accurate, appropriate and compliant.

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will only include pupils for whom permission has been granted by parents/carers.
- Pupils' full names will not be published on the website, particularly in association with photographs.
- Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Parents/carers are reminded of this at key events where they may take photographs e.g. celebration events and assemblies.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Copyright

- The school will seek to ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.

Online Safety Incidents and Concerns

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Symphony Learning Trust, can accept liability for the material accessed, or any consequences of internet access.
- The school will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective.

Addressing potential harms and risks

- The school Online Safety curriculum will address potential risks and harms in three key areas: how to navigate online environments and manage information, how to stay safe online and pupil wellbeing.
- KS1, children are taught to use technology safely and respectfully, keep personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies through programmes such as Purple Mash E-safety units
- KS2, children are taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

- Curriculum content will be regularly reviewed to reflect the different risks that pupils face and remain up to date with current guidance and good practice.
- Teachers will tailor Online Safety lessons to the needs of their pupils in order to provide the most relevant learning experiences.

Monitoring and Reporting

- Online Safety incidents (including cyber-bullying behaviour) will be reported and monitored in line with school procedures, to the Head teacher/ DSL.
- Online Safety incidents of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school safeguarding procedures.

Handling Online Safety Complaints

- Complaints of IT misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher. If this complaint is about the Head teacher, then it must be referred to the school's Chair of Governors.
- Complaints of a child protection nature must be referred to the Designated Safeguarding Leader and dealt with in accordance with school child protection procedures.
- Parents/carers will be informed of the complaints procedure.
- Pupils and parents/carers will be informed of consequences for pupils misusing the internet.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters, and on the school website.
- Parents and carers will, from time to time, be provided with additional information on current Online Safety issues.
- The school will ask all new pupils and parents/carers to sign the Pupil Acceptable Use Policy when the pupil is registered with the school.
- The use of stereotypes will always be challenged.

How to report concerns

- Staff are trained annually on how to report any concerns about online safety such as a child/ren accessing or trying to access inappropriate material online.
- Staff would speak to the DSL or a member of the safeguarding team (or management if unavailable) at the earliest opportunity.
- Staff would report the concern – sharing the name of the child/ren, what had been searched or accessed, the device on which this happens.
- Incidents are logged on CPOMs and tagged under 'e-safety incident/concern'.

Appendix 1 – Acceptable Use Policies

IT Acceptable Use Policy for Pupils

For the purpose of this policy, the 'Head teacher' refers to the Executive Head teacher, Head teacher or Head of School.

To keep me safe whenever I use the internet or email, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer or online equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes or change the settings
- I will not use chat and social media networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own

- I will not take part in harmful online challenges
- I will not take part in cyberbullying
- I will report anything that worries me online to a trusted adult
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website (and is not a hoax)
- I will only use my school email address for log in purposes or in school lesson reasons when instructed to do so by my teacher.

If I break these rules…

- I understand that the school's behaviour guidelines will be followed

I have read and understand this policy and agree to follow it.

Name of pupil _____

Signed _____ Date _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature _____ Date _____

School name: Glen Hills Primary School

.

IT - Acceptable Use Policy Staff and Volunteers

Adopted by Symphony Learning Trust	June 2018
Ratified by Trustees	20th June 2018
Next Review Due	When guidance changes

For the purpose of this policy, the 'Head Teacher' refers to the Executive Head teacher, Head teacher or Head of School.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will,

where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (eg laptops, email, VLE etc). This includes my personal or work mobile phone or tablet if it contains my work email.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will not share or continue to use any logins for any school service or platform when I leave my employment with the Trust.
- I will delete all school data from my personal devices when I leave my employment with the Trust.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the Head teacher/DPO.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer should I leave it unattended.
- I will not allow a third party to access my work emails on my mobile phone or tablet

•

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
- I will not save any personal data to my personal computer.
- I will only use the recommended apps on my personal device for accessing data\emails via G-Suite.
- I will encrypt (Password Protect in most cases) my personal device if I use it to access school personal data or G-Suite apps.
- I will inform the school's Head teacher/ DPO if my personal device e.g. phone or tablet is lost or stolen should it contain any school personal data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the school's retention policy.
- I will not use personal email addresses for work-related purpose.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc). I will not use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School GDPR Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

School: Symphony Learning Trust

Signed: …….. Print name: …….

Date: ……

The authorised persons referred to in this Policy are:

CEO – Mr Tim Sutcliffe

DPO – Mr Daniel Wagg is the DPO for:-

Ashby Hastings Primary School; Fairfield Community Primary School; Glen Hills Primary School; Old Mill Primary School and Symphony Learning Trust

Mrs Donna Hughes is the DPO for:-

Ashby Willesley Primary School; The Meadow Community Primary School; Newcroft Primary School; Orchard Community Primary School and Thornton Primary School

ICT Support provider – Various across the schools

•

IT - Acceptable Use Policy Trustees and Governors

Adopted by Symphony Learning Trust on	1st October 2018
Next Review Due	When guidance changes

For the purpose of this policy, the 'Head Teacher' refers to the Executive Head teacher, Head teacher or Head of School.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- that Governors and Trustees will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that Governors and Trustees will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect Governors and Trustees to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (eg laptops, email, VLE etc). This includes my personal or work mobile phone or tablet if it contains my work email.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will not share or continue to use any logins for any school service or platform when I leave my employment with the Trust.
- I will delete all school data from my personal devices when I leave my employment with the Trust.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the Head teacher/DPO

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer should I leave it unattended.

- I will not allow a third party to access my work emails on my mobile phone or tablet

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
- I will not save any personal data to my personal computer.
- I will only use the recommended apps on my personal device for accessing data\emails via G-Suite.
- I will encrypt (Password Protect in most cases) my personal device if I use it to access school personal data or G-Suite apps.
- I will inform the school's Head teacher/DPO if my personal device e.g. phone or tablet is lost or stolen should it contain any school personal data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the school's retention policy.
- I will not use personal email addresses for work-related purpose.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc). I will not use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School GDPR Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

School: Symphony Learning Trust

Signed: …….. Print name: …….

Date: ……

The authorised persons referred to in this Policy are:

CEO – Mr Tim Sutcliffe

DPO – Mr Daniel Wagg is the DPO for:-

Ashby Hastings Primary School; Fairfield Community Primary School; Glen Hills Primary School; Old Mill Primary School and Symphony Learning Trust

DPO - Mrs Donna Hughes is the DPO for:-

Ashby Willesley Primary School; The Meadow Community Primary School; Newcroft Primary School; Orchard Community Primary School and Thornton Primary School

ICT Support provider – Various across the schools

•

Appendix 2 – Responding to Online Safety Incident