Pott Shrigley Church School

Shrigley Road, Pott Shrigley, Cheshire
SK10 5RT
Tel: 01625 573260
e-mail: admin@pottshrigley.cheshire.sch.uk
Headteacher: Mrs Anne-Marie Willis

Online safety Policy Autumn 2023

Contents

'Be kind and compassionate to one another, forgiving each other, just as in Christ, God forgave you'
Ephesians 4:32

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

<u>The 4 key categories of risk</u>

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, Keeping children safe in education - GOV.UK (www.gov.uk) and its advice for schools on:

- Teaching online safety in schools Teaching online safety in schools - GOV.UK (www.gov.uk)
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff Preventing bullying - GOV.UK (www.gov.uk)
  Preventing bullying - GOV.UK (www.gov.uk)
- Relationships and sex education Relationships and sex education (RSE) and health education - GOV.UK (www.gov.uk)
- Searching, screening and confiscation Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)

It also refers to the DfE's guidance on protecting children from radicalisation. The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk)

It reflects existing legislation, including but not limited to the Education Act 1996 Education Act 1996 (legislation.gov.uk) (as amended), the Education and Inspections Act 2006 Education and Inspections Act 2006 (legislation.gov.uk)and the Equality Act 2010 Equality Act 2010 (legislation.gov.uk)

In addition, it reflects the Education Act 2011, Education Act 2011 (legislation.gov.uk)which has given teachers stronger powers to tackle cyber bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will ensure the safeguarding governor as part of safeguarding visits monitors online safety. The governor responsible for safeguarding is Jane Langdon.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Do all that they reasonably can to limit children's exposure to the risks identified in the 4C's from the school's IT system. The governing body will ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an

awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The governing body will consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with staff, as necessary, to address any online safety issues or incidents
- Working with the staff, as necessary, to ensure the appropriate filtering and monitoring systems are in place and reviewed regularly.
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy.
- Ensuring that any online safety incidents are logged in line with the child protection and safeguarding policy (CPOMs).
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety to the governing board.

3.4 ICT support

ICT support is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems.

- Alongside the service provider blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

3.5 All staff and volunteers

- All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged in line with the child protection and safeguarding policy (CPOMs).
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:
Notify a member of staff or the headteacher of any concerns or queries regarding this policy
Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
Parents can seek further guidance on keeping children safe online from the following organisations and websites:
What are the issues? – What are the issues? - UK Safer Internet Centre
Hot topics – Help & advice | Childnet
Parent resource sheet – Help & advice | Childnet

3.7 Pupils

Pupils are expected to:

- Adhere to the Acceptable use agreement
- Seek help from school staff if they have any concerns
- Report online safety incidents and concerns

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:
Relationships and sex education (RSE) and health education - GOV.UK (www.gov.uk)
In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping 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.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in information via our website
This policy will also be shared with parents.
Online safety may also be covered during parents' evenings and parent workshops

The school will let parents know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites.
Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Types of cyber bullying may include:

- Child on child sexual abuse and harassment.
- Threatening, facilitating or encouraging sexual violence. Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts. Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery. Abuse between young people in intimate relationships online).
- Grooming and exploitation - Where an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing.
- Child sexual exploitation (CSE) and child criminal exploitation (CCE). CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

- CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
- Radicalisation, the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.
- Online hoaxes and harmful online challenges - An online hoax is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. Harmful online challenges refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.
- An online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

6.2 Preventing and addressing cyber-bullying

School has a zero tolerance approach to any forms of cyber bullying.To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation
- Authorised staff members may examine, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence
- If inappropriate material is found on the device, it is up to headteacher to decide on a suitable response.
- If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable.
- If the material is not suspected to be evidence in relation to an offence, staff members may delete it if: They reasonably suspect that its continued existence is likely to cause harm to any person, and/or The pupil and/or the parent refuses to delete the material themselves.

- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- Not view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next.
- The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation Searching, screening and confiscation in schools - GOV.UK (www.gov.uk) and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

If it is deemed essential pupils in Years 5 and 6 may bring mobile devices into school, but are not permitted to use them whilst in school this includes during:

Lessons.

Clubs before or after school, or any other activities organised by the school.

All devices must be handed in to the class teacher on entry to school and can be retrieved at the end of the school day.

School will accept no responsibility for loss or damage to any devices.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation/banning of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring any removable hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the ICT support.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on online safety and links to child protection and safeguarding.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through:
  o Abusive, harassing, and misogynistic messages
  o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially
  around chat groups
  o Sharing of abusive images and pornography, to those who don't want to receive such content
  Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:
• Develop better awareness to assist in spotting the signs and symptoms of online abuse.
• Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
• Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements
The DSL logs behaviour and safeguarding issues related to online safety as per the schools child protection and safeguarding policy.
This policy will be reviewed every year by the head teacher. The policy will be shared with the governing body.

13. Links with other policies
This online safety policy is linked to our:
Child protection and safeguarding policy KCSiE
Behaviour policy
Staff disciplinary procedures
Data protection policy and privacy notices
Complaints procedure
ICT and internet acceptable use policy

Appendix 1

Key stage 1 online agreement

This is how we stay safe when we use computers:

I ask an adult when I want to use the computer.

I take care of the computer and other equipment.

I ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Child’s name	
Parent’s name	
Signed	
Date	

Appendix 2

Key stage 2 online agreement

I understand that I must use the school's ICT systems in a responsible way, to ensure that there is no risk to my safety, the safety of my friends and other children in the school and the ICT systems

For my own personal safety:

- I understand the school monitors use of the ICT systems, emails and other digital communications.
- I treat my username and password like my toothbrush – I don't share it, and I don't try to use someone else's.
- I am aware of 'stranger danger' when communicating online.
- I do not disclose or share personal information (like my name, address, school name, phone number, etc.) – either my own or someone else's – when online.
- If I arrange to meet people off-line that I have communicated with online, I will tell an adult what I am doing, arrange to meet in a public place and take an adult with me.
- I will immediately report anything that makes me uncomfortable, sad, afraid or angry that I see online, on my phone/other device.

I understand that everyone has an equal right to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up room and prevent other people from carrying out their work.
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing or video broadcasting (unless the video broadcasting has been agreed with my teacher).
- I will act as I expect others to act towards me.

When using the internet, I will:

- ensure I have permission to use other people's original work in my own work.
- not try to download copies of music or videos that are not my own.
- take care to check that the information I access is accurate, as I understand that the work of others may not be truthful.

I am responsible for my actions, in and out of school. I understand that the school has a right to take action if I am involved in incidents when I am out of school and where they are about my membership of the school community (e.g., cyber-bullying, using images of myself, friends, other children, teachers or other adults; sharing other people's personal information, etc.)

I agree to follow these guidelines when:

- I use the school ICT systems and equipment
- I use my own equipment in school where this is allowed (e.g., my camera at school parties, etc.)
- I use my own equipment out of school in a safe and responsible way as I have been taught in school.

Child's name	
Signed	
Date	

Appendix 3

Parental online agreement

We have an Acceptable Use Agreement in place to safeguard children in their use of technologies such as the internet, mobile phones, digital devices, etc.

We want to ensure that:
children will be responsible users and stay safe while using the internet and other communication technologies (for educational, personal and recreational use).
school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
parents/carers are aware of the importance of e-safety and are involved in the education and guidance of their children with regard to their online behaviour.

Pott Shrigley Church school will ensure that our children have good access to ICT to enhance their learning and expect that they agree to be responsible users. A copy of the Child Acceptable Use Agreement is attached, so that you as a parent/carer are aware of the school expectations of the children in our care.

As the parent/carer of a child at Pott Shrigley Church school, I:

- know that my child has signed an Acceptable Use Agreement and receives e-safety education to help them understand the importance of safe use of ICT – both in and out of school.
- understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems.
- understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have any concerns about possible breaches of the Acceptable Use Agreement
- encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Child's/children's names		
Parents name		
Signed		
Date		

Appendix 4

Staff Acceptable Use Policy (Autumn 2023)

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.
To ensure that members of staff are fully aware of their professional responsibilities when using Information Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that IT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email, instant messaging and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters and is only used on one system and is changed regularly at least once a term).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Headteacher.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and GDPR regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the School Shared area to upload any work documents and files. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces .

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead and the technician as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Head teacher or IT support asap.

13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved

communication channels e.g. via a school provided
email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking

or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head teacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of IT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP (Acceptable Use Policy) and the Law.

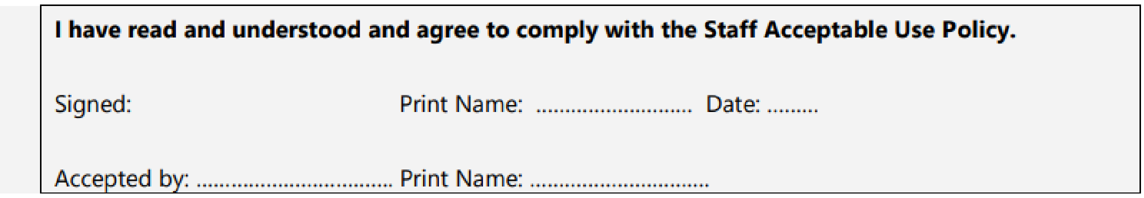
15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead or Deputies.

18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

19. I ensure that my mobile phone is turned to silent and kept in my bag/desk drawer during lesson time. I will not use my mobile phone to take photographs or store images of children.



I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: Print Name: .... Date: ....

Accepted by: .... Print Name: ....