St Mary's CE Primary School

N8 7QN

Online Safety Policy

(Including Acceptable Use Guidance)

2022

Jesus said, "Love one another as I have loved you." (John 15:12)

Our Vision

As we love, we flourish

As we flourish, we aspire

As we aspire, we achieve

Together, we are a family.

Friendship, Compassion, Hope, Wisdom, Community, Endurance.

January 2022

Through our daily school life at St Mary's Church of England Primary School we encourage our children to build respectful friendships and demonstrate compassion towards others. Through this we build a strong community spirit, as together we are a family. Our teaching and learning provides the children with the wisdom and endurance they need to expand their minds socially, morally and academically so allowing them to achieve and flourish and fulfil 'Life in all its Fullness.' (John 10:10). We encourage our children to demonstrate and develop a dignity in their work and themselves which enables them to hope to aspire to be the best they can possibly be.

E Safety and Internet Usage

1. **Aims**

Our school aims to:

- Have robust processes in place to ensure the online safety of children, 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.
- Ensure students are educated in how to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact.
- Establish clear mechanisms to intervene and escalate an incident, where appropriate.

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The 4 key categories of risk

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, anti-Semitism, 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 semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Links with other policies

The school's E-Safety Policy will operate in conjunction with other policies including those for Computing, Positive Behaviour, Anti-Bullying, Safeguarding and Child Protection, Data Protection and Peer-on-Peer Abuse Policy.

2. **Background - Why Is Internet Use Important?**
   The purpose of internet use in school is to raise educational standards, to promote children achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

   Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business, and social interaction. Access to the internet is therefore an entitlement for children who show a responsible and mature approach to its use and St Mary's has a duty to provide children with quality internet access.

   Many children will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

3. **How Does Internet Use Benefit Education?**
   Benefits of using the internet in education include
   - Access to world-wide educational resources including museums, libraries, and art galleries.
   - Rapid and cost-effective worldwide communication.
   - Inclusion in the National Education Network which connects all UK schools (LGfL).
   - Educational and cultural exchanges between children worldwide.
   - Access to experts in many fields for children and staff.
   - Professional development for staff through access to national developments, educational materials, and effective curriculum practice.
   - Collaboration across support services and professional associations.
   - Improved access to technical support including remote management of networks and automatic system updates.
   - Exchange of curriculum and administration data with the Local Authority.
   - Access to learning wherever and whenever convenient.
   - Greatly increased skills in literacy.
   - In times of lockdowns and COVID 19, internet access allows students to continue learning remotely.

4. **How Can Internet Use Enhance Learning?**
   - The school internet access is designed expressly for children use and includes filtering appropriate to the age of our children.
   - Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use in line with Computing Policy and NC objectives.
   - Internet access will be planned to enrich and extend learning activities.
   - Staff will guide children in online activities that will support learning outcomes planned for the children' age and maturity.
   - Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation in line with Computing policy and NC objectives.

5. **Good Habits**
   E safety depends on effective practice at several levels:
   - Responsible ICT use by all staff and children; encouraged by education and made explicit through published policies.
   - Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network / LGfL standards and specifications.

6. Dangers To Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyberbullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy, and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The E safety policy that follows explains how we intend to do this.

7. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on children' 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.

8. Roles and responsibilities

8.1 The governing body

The Resources Committee of the Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

- The governor who oversees online safety is Stuart Goldberg.
- All governors will ensure that they have read and understood this policy and will adhere to the terms of it and the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).

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

8.3 The Designated Safeguarding Lead (DSL)
Details of the school's DSL are set out in our Child Protection and Safeguarding Policy.
The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged either using 'Integris' or 'My Concern' and dealt with appropriately in line with this policy
- 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 in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

8.4 External ICT support
We currently outsource ICT to a third party company (CNETSO)
The ICT manager is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children 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 monthly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

8.5 All staff
All staff, including contractors and agency staff, and volunteers who undertake regular activities at school will:
- Ensure that they have read and understood this policy
- Adhere to the terms of it and the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).
- Work with the DSL to ensure that any online safety incidents are logged on using 'Integris' or 'My Concern' as appropriate and dealt with appropriately in line with this policy

- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Staff will have regular updates and training on E-Safety requirements

This list is not intended to be exhaustive.

8.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Adhere to the terms of it and the acceptable use guidance for parents and carers (Appendix 1 or 2 depending on the Key Stage their child is in).
- Ensure their child is aware of and adheres to the terms of this policy and the acceptable use guidance for children (Appendix 1 or 2 depending on the Key Stage their child is in).
- Parents should consult the E-Safety section of the school website, which gives further guidance on keeping children safe online, and giving links to several useful organisations.
  - Parents' attention will be drawn to the E-safety Policy and expectations/guidance in newsletters, communication home and on the school website.
  - Parents will receive a copy of their child's Acceptable Use Agreement.

8.7 Visitors and members of the community

All visitors to the school will, where appropriate:

- Be made aware of this policy via our school website, and, if appropriate, be given a copy of the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).

8.8 Children

- Children will be made aware of the acceptable use guidance for children (Appendix 1 and 2) during lessons, assemblies and workshops.
- Rules for internet access will be posted in all classrooms.
- Children will be informed that internet use will be monitored.
- Children will be reminded of E safety rules regularly – especially when using the internet.

9 Email & Online Collaboration

- Children may only use approved email accounts on the school system.
- LGfL USO accounts have been created for each child at St Mary's Primary with enhanced safeguarding measures in place to ensure our children's safety as much as possible.
- Children must immediately tell a teacher if they receive offensive messages.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Children must not access others children's accounts or files.
- Whole class or group email addresses should be used in school.
- Children must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Children must not deliberately seek out offensive materials. Should any children encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.

- Children are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Children must ask permission before accessing the internet and have a clear idea of why they are using it.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses.
- Children must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain letters is not permitted.
- Children must sign an agreement form if using school device at home which includes a code of conduct.

10 Social Networking

- At St Marys we block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Children are advised never to give out personal details of any kind which may identify them or their location.
- Children are advised not to place personal photos on any social network space.
- Children are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Children are encouraged to invite known friends only and deny access to others
- Children and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old.

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never** add children as 'friends' into their personal accounts (including past children under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, children, parents or colleagues including members of the governing body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current national teacher's standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action

11 Filtering

The school will work in partnership with CNETSO and LGfL, our I.T. support provider and internet Service Provider respectively, to ensure filtering systems are as effective as possible.

12 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Please see our Data Protection policy.

13 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. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the E safety policy is adequate and that the implementation of the E safety policy is appropriate.

14 Handling E safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Children and parents will be informed of the complaints procedure.

15 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and their risks assessed.

16 Use of Communication and Information Technology In School (Mobile Phones)

- Only Y5 and Y6 children who are independent travellers to and from school are allowed to bring their phones to school.
- Phones must be handed over to the teacher for safe keeping throughout the entire day and will be returned to the child at the end of the day.

17 When using email, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email or electronic message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents must be professional in tone and content
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

18 Educating children about online safety

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

In **Key Stage 1,** children 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

Children 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**, children 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*
- *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.

19 Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
- Online safety will also be covered during parents' evenings.
- As part of Safer Internet Day, an E-safety talk will be held, raising awareness and offering advice or support.
- 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.

23. Sexting

- The consensual and non-consensual sharing of nude and semi-nude images, videos and livestreams (otherwise known as sexting or youth-produced sexual imagery) counts as unacceptable use of ICT and internet.
- The school will always consider an incident such as this as a serious safeguarding issue, and will refer the case via the DSL to the appropriate authorities, including the police.

24. Cyber-bullying

23.1 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 one person or group by another person or group, where the relationship involves an imbalance of power.

23.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes as well as within discrete curriculum-based E-Safety lessons.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training (see section 11 for more detail).
- Information on school website and content of Safer Internet Day presentation on cyber-bullying to parents helps them become aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Positive Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among children, the school will use all reasonable endeavours to ensure the incident is contained.
- The Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

26.3 Examining electronic devices

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on children' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
    - Cause harm, and/or
    - Disrupt teaching, and/or
    - Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
    - Delete that material, or
    - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
    - Report it to the police
- Any searching of children will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

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

24. Staff using work devices outside of 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 their 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 – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use guidance, 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 computing lead or ICT Manager (CNETSO).

25. How the school will respond to issues of misuse

- Where a children misuses the school's ICT systems or internet, 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 Policy. 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.

26. Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- 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 (for example through emails and staff meetings).
- 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.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

Appendix 1: EYFS and KS1 acceptable use guidance - children and parents/carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR CHILDREN AND PARENTS/CARERS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I am aware that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 2: KS2 - acceptable use guidance for children and parents/carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR CHILDREN AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission.
- I will hand my phone in to my class teacher at the beginning of the day and it will be locked away by the teacher until home time
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I know that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 3: acceptable use guidance for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of children without checking with teachers first • Share confidential information about the school, its children or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will: • Only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • Let the designated safeguarding lead (DSL) and ICT manager know if a children informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • Always use the school's ICT systems and internet responsibly, and ensure that children in my care do so too. **I know:** • That the school will monitor the websites I visit and my use of the school's ICT facilities and systems.