Online Safety and Acceptable Use of Devices Policy

Capel St. Mary CEVC Primary School

The Street, Capel St Mary, Ipswich, Suffolk IP9 2EG

Tel: 01473 310386
E:mail **admin@capel-st-mary.suffolk.sch.uk**
Website: www.capel-st-mary.suffolk.sch.uk

Care
Achieve
Persevere
Enjoy
Learn

Suffolk County Council

1. Aims

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation and technology often provides the platform that facilitates such harm.

The governing body has had due regard to the additional information and support set out in KCSiE 2025 and ensures that the school has a whole school approach to online safety and has a clear policy on use of communications technology in school. Online safety will be a running and interrelated theme when devising and implementing policies and procedures. This will include considering how online safety is reflected in all relevant policies and whilst planning the curriculum, any teacher training, the role of the DSL and any parental engagement.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school adopts a whole school approach to online safety to protect and educate pupils and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns as appropriate.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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

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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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 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, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education (RSE) and health 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 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 co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is the Named Governor for Safeguarding.

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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

3.2 The Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and alternate DSLs are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and governing body to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged on CPOMS (the school's online safeguarding recording system) and dealt with appropriately in line with this policy
- Making sure 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 as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing body
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety (via email, e-bulletins, staff meetings or training sessions), to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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 making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of the need to report any incidents of those systems or processes failing to the DSL or ICT Manager as soon as possible for investigation/action/sanction
- Following the correct procedures by liaising with the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents, e.g. suspected misuse of school devices or the internet, are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure 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/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Make sure that 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 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 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

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

Learning about online safety through theme days, such as Safer Internet Day, and it is embedded into the Personal, Social, Health and Economic Education (PSHE), computing and the broader curriculum. For example, pupils will learn about online safety in relation to the theme of bullying in PSHE.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private, including passwords
- Identify where to go for help and support when they are uncomfortable and have concerns about content or contact on the internet or other online technologies; this includes the idea of blocking or reporting other users
- Understand the benefits of limiting time online as part of a balanced lifestyle to support wellbeing

Pupils in **Key Stage (KS) 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
- Be discerning in evaluating digital content
- Understand the benefits of limiting time online as part of a balanced lifestyle to support wellbeing

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

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.

4.2 Pupils will be taught practical cyber security skills

In line with the DfE's non-statutory cyber security standards for schools and colleges, all pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack

- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and/or Class Dojo. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers 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/carers 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. (See also the school behaviour policy.)

6.2 Preventing and addressing 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 encourage them 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. Class teachers will discuss cyber-bullying with their classes.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are 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 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 other senior leaders, 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, a DSL or another senior leader
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, 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 the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team 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 whether 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/carer 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 (or equivalent) 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 and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

The behaviour policy sets out information about searching and confiscation.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots, such as ChatGPT and Google Gemini.

Capel St Mary CEVC Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Capel St Mary CEVC Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Staff members may use AI tools, such as ChatGPT, to generate learning content that does not include the personal data of pupils or staff members. For example, AI tools may be used to generate quizzes that support pupils' recall and retrieval of previously learned content. Furthermore, AI tools may be used by staff members to analyse non-personal data, such as anonymised survey data. The school recognises the benefits for workload and efficiency of using technology to generate content or complete administrative tasks quickly. Staff members should, however, make reasonable checks to ensure that the content is accurate, does not mislead and is not offensive.

7. Filtering and Monitoring

The school will ensure that there are appropriate filters and monitoring systems in place to safeguard children and young people from potentially harmful and inappropriate online material.

At Capel St Mary CEVC Primary School we use SENSO software which sends alerts to the Headteacher and the School's ICT Manager, Mrs Shirley Overton, should a key word or individual key strokes indicate that a child is accessing inappropriate material. We also use Fortinet software which prevents both children and staff accessing inappropriate websites. The type and nature of blocked sites are reviewed so that sites which may have educational use (such as teachers accessing YouTube videos) are not blocked as standard. Mrs Shirley Overton also receives a report where an inappropriate website has attempted to be accessed. These systems are in place through contracted broadband and internet services.

The Department for Education's filtering and monitoring standards set out that schools and colleges should:
• identify and assign roles and responsibilities to manage filtering and monitoring systems.
• review filtering and monitoring provision at least annually.
• block harmful and inappropriate content without unreasonably impacting teaching and learning.
• have effective monitoring strategies in place that meet their safeguarding needs.

The Department for Education has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely and explains how filtering and monitoring requirements apply to the use of generative AI in education.

8. Acceptable use of the internet and devices in school

Internet users must not display, access, use, extract, store, distribute, print, reveal or otherwise process any kind of image, document or other material which is sexually explicit or offensive in any other way, on any school system. This includes but not limited to, sending obscene emails, gambling, and viewing pornography or other inappropriate content. This activity would be a violation of the school's Safeguarding and Online Safety and Acceptable Use of Devices Policy and would be considered to be examples of serious misconduct.

All pupils, parents/carers, 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 and devices must be for educational or work purposes only, or for the purpose of fulfilling the duties of an individual's role unless special permission has been given by a senior leader. Personal websites, particularly social networking sites, should not be accessed via computers at school.

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

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

Unacceptable use:

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in the school's disciplinary policy being applied.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher (or Deputy Headteacher / Senior Teacher in the Headteacher's absence) will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Personal use of school ICT systems

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or may restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with pupils, parents or professional colleagues, e.g. during lessons or training sessions;
- Does not constitute 'unacceptable use' (see above);

- Takes place when no pupils are present;
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes;
- Does not impact on work efficiency or costs;
- The level of use is reasonable (as determined by the Headteacher) and not detrimental to the main purpose for which the facilities are provided;
- Is not of a commercial or profit-making nature;
- Is not of a nature that competes with the business interests of the school or conflicts with an employee's obligations.

Staff should exercise caution in using the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos), and must ensure any such use is in line with the Staff Code of Conduct. They must also be cautious about downloading apps or materials that may have viruses and should seek guidance from the ICT Manager if necessary.

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (i.e. filtering and monitoring systems). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices, such as mobile phones, smart watches or tablets (see section 13 below) in line with the school's Code of Conduct and provided that personal devices are not used for unacceptable purposes as defined above and in the acceptable use agreement (Appendix 3). Personal devices should only be used according to the principles outlined above in relation to the school's ICT facilities.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see the Staff Code of Conduct) and use of email to protect themselves online and avoid compromising their professional integrity.

9. Pupils using mobile devices in school

Pupils may not bring personal mobile devices into school, unless they are specifically approved on a case-by-case basis and a mobile phone permission slip has been completed by the parent. Any mobile device brought into school by a pupil should be turned off and placed in the school office at the beginning of the school day and can only be collected at the end of the school day. The school does not take any responsibility for the loss or damage of these devices.

Smart watches which can connect to the internet through a SIM card that can also make calls must not be worn by pupils.

Pupils must not use mobile phones, or other such devices, during:

- Lessons
- Break or lunch time
- Clubs before or after school, or any other activities organised by the school

Exceptions may be granted on medical grounds, such as devices that measure blood sugar levels, or in special educational circumstances when a specific device may help a pupil access the curriculum due to their particular needs. This is the Headteacher's discretion. If a pupil is allowed to bring a device into school, they must comply with guidelines regarding acceptable use and it must not disrupt their, or others', learning. Pupils must not distribute photos, videos or audio recording created in school.

Pupils bring their personal ICT devices to use school at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Capel St Mary Primary School is in no way responsible for:

- Personal devices that are broken whilst at school or during school-sponsored activities.
- Any data lost on personal devices.
- Personal devices that are lost or stolen at school or during school-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues, Portable Appliance Testing).
- Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). 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 of their device.

10. 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, in combination with numbers and special characters
- 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
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that 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 Manager.

11. 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 on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. The incident will be recorded on CPOMS, so that online safety concerns are reflected in the pupil's safeguarding chronology.

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 code of conduct and, if necessary, the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. Training for staff, governors and volunteers

All new staff members will receive training, as part of their safeguarding training, on safe internet use and online safeguarding issues, including acceptable use of portable devices, 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, e-bulletins and staff meetings).

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

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 and alternate DSLs 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.

13. School social media accounts

The school has official social media accounts, e.g. a Facebook page, managed by a staff member who has been authorised by the Headteacher to do so. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The guidelines below set out what can and cannot be posted on the school's social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool requires the approval of the Headteacher. Users must not set up social media sites or channels seeking to represent the school without this approval. The Headteacher may restrict or stop the use of official social media sites at any time at their discretion.
- Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with relevant school policies and must not be used for 'unacceptable' purposes as defined in this policy or at the discretion of the Headteacher.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Written parental consent will be obtained, as required, for use of pupils' data (such as photographs) in social media communications and posts.

- All social media communications and posts must be respectful of all members of the school community and should not be used to make complaints. Any complaints must be made according to the formal procedures for this.
- Staff members should not enter into ongoing dialogue with other social media users. Social media communications are only to be used for posting official school news or information.

14. Use of Photos / Videos of Staff Members

At Capel St Mary CEVC Primary School, we sometimes take photographs / videos of staff. We use these photos for a range of purposes. For example, photos including staff members appear on our website, on internal displays and on social media to share information about school activities. Photos may be used on posters about employees' roles in school. These purposes for sharing photos are a necessary part of the school's work and this data is shared on the lawful basis of 'Public Task'. We also use photos for marketing purposes, such as on advertisements and in our prospectus. On these occasions, we process images of staff members on the lawful basis of 'Legitimate Interests'. We value using staff photos, not only for transparency to parents as to identify who staff are, but also for ease of identification for safeguarding purposes and to celebrate the curriculum and enrichment opportunities in school. If staff members wish to opt out of us using your images for any of the reasons mentioned above you may do so at any time. Please contact the Headteacher.

15. The Use of Personal Devices in School: Staff Members, Visitors and Volunteers

15.1 Introduction

Capel St Mary CEVC Primary School recognises the benefits of mobile technology and is committed to supporting staff members, visitors and volunteers in the acceptable use of personal devices. A 'personal device' is any device that is internet-enabled via Wi-Fi or mobile networks, such as mobile phones, tablets or wearable technology, including smart watches.

As with all personal possessions, the school is not responsible for the security of personal mobile phones. Staff members must be sensitive about their roles in school and mobile phones should only be used at appropriate times.

- Phones should be silent during lesson times.
- Employees should not make or receive calls in front of pupils or during lesson times or during times when they are expected to be working (i.e. not break times).
- Phones should not be used to record and keep images or footage of pupils.

It is recognised that imposing rigid regulations or 'bans' can be counterproductive and can lead to a culture of secrecy, suspicion and uncertainty. Therefore, this code operates on a basis of professional trust with regard to the use of personal mobile phones. There may be times when exceptional personal circumstances require more flexibility. This should be negotiated with a line manager or the Headteacher.

Staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of school information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- Report the loss of any device containing school information, or any security breach immediately to the Data Protection Officer.
- Ensure that no school information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of / sold / transferred to a third party.

Visitors and volunteers will:

- Familiarise themselves with the use of personal devices at the school.
- Only use personal devices for agreed purposes and with parental or the relevant permission.
- Not share information from personal devices via social media and will not keep school information indefinitely.

15.2 Detailed Arrangements & Procedures

Use of personal devices at the school

Staff should only use their mobile phones at appropriate times of the day, e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images, videos or audio recordings of pupils or staff, except in special circumstances, e.g. school equipment is unavailable and there is a clear benefit from doing so. This should only be done with the permission of a senior leader and when parental consent has been received from parents / carers.

In addition, visitors and volunteers must follow this policy. It is not acceptable for visitors or volunteers to bring recording equipment into the school.

The school reserves the right to refuse staff, visitors and volunteers permission to use their own device on school premises.

Use of cameras and audio recording equipment

In accordance with guidance from the Information Commissioner's Office (ICO), parents/carers are welcome to take videos and digital images of their children at school events (including school organised activities out of school) on their personal equipment for their own personal use. To respect everyone's privacy, members of staff should make parents/carers aware that these images / recordings (in particular images including children who are not their own) must not be published/made publicly available whether on social networking sites or otherwise.

Teaching and support staff are allowed to take digital/video images to support educational aims. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the school into disrepute.

Photographs/video published on the school's websites, or elsewhere, which include pupils will be selected carefully and permission will be sought from the relevant parent/carer. The names of pupils who appear on images/video will not be published, other than with the prior, explicit consent of the parent/carer.

Video conferencing is a tool which the school may use to support learning, for example during a period of school closure. Permission for this will be sought from parents/carers prior to this taking place. The school may make recordings of video conferences to support educational aims. Where a video conference involves participants from outside of the school, permission must be requested in advance of making a recording. Video conferencing is always supervised by a competent adult, who knows how to end the call if necessary. The adult who supervises the call is responsible for switching off the camera at the end of the call.

Other visitors are not generally expected to use their own personal devices to take photographs, video, or audio recordings in school. In exceptional circumstances, they may do so, provided they have checked that parental consent has been received by the school. This includes people who may be identifiable in the background. They must also have the explicit permission of a senior leader.

Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the school's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school network.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

Access to the schools' internet connection

The school provides a wireless network that staff and visitors to the school may use to connect their personal devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access for anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's network. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

Access to the school's systems

Staff are permitted to connect to or access the following school services from their device:

- The school email system.
- The school management information system.
- School-approved apps, e.g., Class Dojo for communication.

Staff may use the systems to view school information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their personal devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the school as soon as possible.

Staff must not send school information to their personal email accounts.

Monitoring the use of personal devices

The school may use technology that detects and monitors the use of personal and other electronic or communication devices which are connected to or logged on to the school's wireless network or IT systems. By using a device on the school's network, staff and visitors agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school as soon as possible.

Security of staff personal devices

Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up-to-date.

Staff must ensure that passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used.

Support

The school takes no responsibility for supporting staff's own devices, nor does the school have a responsibility for conducting annual PAT testing of personal devices. However, the school will support staff in ensuring that they have appropriate levels of security in place.

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, the school's disciplinary policy will be applied.

Incidents and reporting

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the school's Data Protection Officer. However, the school does not accept responsibility for damage or loss of personal devices in school.

16. Social Media Platforms and Digital Networking

When using social networking sites, staff members must be conscious of the overlap of 'personal' and 'professional' profiles online. If Staff members have a personal profile on social media sites, they should consider not using their full name, as pupils may be able to find them. Staff may consider using a first and middle name instead and consider setting up public profiles to private. Staff members must not post any comments, photographs, images or conversations on social networking websites which may bring themselves or the school into disrepute. Staff members must not become 'friends' with pupils on social networking sites and must exercise extreme caution in their online relationships with parents. Security settings should be maintained at the highest level in order to prevent members of the public seeing any of your personal information. Adults in a position of trust should refrain from online communications with pupils, except where this is for professional purposes, such as setting homework electronically. Staff must not post any images online that identify children who are pupils at the school without appropriate consent.

17. Monitoring arrangements

Staff members log behaviour and safeguarding issues related to online safety on CPOMS. The DSL will review online safety issues with other trained DSLs and the ICT Manager. This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing body.

18. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures

- Data protection policy and privacy notices
- Complaints procedure
- Staff Code of Conduct

Appendix 1:

Key Stage 1 Online Safety & Device Use Agreement (Pupils & Parents / Carers)

(Tick and sign together)

Pupil

My teacher or grown-up has talked to me about how to stay safe when using computers, tablets, or the internet at school.

I understand that I should:

- ☐ Ask an adult before using the internet
- ☐ Be kind and polite online
- ☐ Keep my password secret
- ☐ Tell an adult if something online makes me feel worried or unhappy

Pupil name: _____ **Class:** _____

Pupil signature (or mark): _____ **Date:** _____

Parent / Carer

I have talked with my child about staying safe online and understand the school's expectations. I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree that I will:

- ☐ Support the school's Online Safety and Acceptable Use Policy
- ☐ Help my child to use technology safely and responsibly
- ☐ Encourage my child to tell an adult if they are worried about something online

Parent / Carer name: _____ **Signature:** _____

Date: _____

Appendix 2:

Key Stage 2 Online Safety & Device Use Agreement (Pupils & Parents / Carers)

(Tick and sign together)

Pupil

My teacher has explained how to stay safe and responsible when using the internet, school devices, and online services.

I understand that I should:

- ☐ Only use the internet and devices when a teacher allows me to
- ☐ Use approved websites, apps, and online tools
- ☐ Keep my username and password private
- ☐ Keep my personal information safe
- ☐ Be kind, polite, and respectful online
- ☐ Not open links or files from people I do not know
- ☐ Tell a trusted adult if something online makes me feel worried, uncomfortable, or unsafe

I agree to follow these rules to help keep myself and others safe.

Pupil name: _____ **Class:** _____

Pupil signature: _____ **Date:** _____

Parent / Carer

I have discussed online safety with my child and understand the school's expectations for the safe and responsible use of technology. I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree that I will:

- ☐ Support the school's Online Safety and Acceptable Use Policy
- ☐ Encourage safe, responsible, and respectful online behaviour
- ☐ Reinforce the importance of keeping personal information and passwords private
- ☐ Encourage my child to report any online concerns to a trusted adult
- ☐ Work with the school if any online safety issues arise

Parent / Carer name: _____ **Signature:** _____

Date: _____

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
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 that 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 pupils without checking with teachers first • Share confidential information about the school, its pupils 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. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will 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. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	