



MERSHAM PRIMARY SCHOOL

# Online Safety Policy

Date reviewed/updated	May 2025
Next review date	May 2026

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

**Designated Safeguarding Lead:** Cheryl Chalkley - Headteacher

**Signed:** ----- **Date:** -----

**Governor with Lead Responsibility:** Lesley Caldwell - Chair of Governors

**Signed:** ----- **Date:** -----

# Contents

<b>1. Policy Aims.....</b>	<b>3</b>
The 4 key categories of risk.....	3
<b>2. Legislation and guidance.....</b>	<b>3</b>
<b>3. Roles and Responsibilities.....</b>	<b>3</b>
3.1 The Governing Board.....	4
3.2 The Headteacher.....	4
3.3 The Designated Safeguarding Lead (DSL).....	4
3.4 The ICT Manager.....	5
3.5 All Staff and Volunteers.....	5
3.6 Parents/Carers.....	6
3.7 Visitors and Members of the Community.....	6
<b>4. Educating Pupils About Online Safety.....</b>	<b>6</b>
4.1 Safer Use of Technology - See also Acceptable Use Policies.....	6
4.1.1 Classroom Use.....	6
4.2 In Key Stage (KS) 1, pupils will be taught to:.....	7
4.3 Pupils in Key Stage (KS) 2 will be taught to:.....	7
4.4 By the end of primary school, pupils will know:.....	7
4.5 Vulnerable Learners.....	7
<b>5. Educating Parents/Carers About Online Safety.....</b>	<b>8</b>
<b>6. Cyber-Bullying.....</b>	<b>8</b>
6.1 Definition.....	8
6.2 Preventing and addressing cyber-bullying.....	8
6.3 Examining electronic devices.....	9
6.4 Artificial intelligence (AI).....	10
<b>7. Acceptable use of the internet in school.....</b>	<b>10</b>
7.1 Filtering and Monitoring.....	10
7.1.1 Filtering.....	10
7.1.2 Monitoring.....	11
<b>8. Security and Management of Information Systems.....</b>	<b>11</b>
8.1 Password Policy.....	11
8.2 Managing the Safety of our Website.....	11
8.3 Managing Email.....	12
8.3.1 Staff email.....	12
<b>9. Pupils using mobile devices in school.....</b>	<b>12</b>
<b>10. Staff using work devices outside school.....</b>	<b>12</b>
<b>11. How the school will respond to issues of misuse.....</b>	<b>13</b>
<b>12. Training.....</b>	<b>13</b>
12.1 Staff, governors and volunteers.....	13
12.2 Pupils.....	14
<b>13. Monitoring arrangements.....</b>	<b>14</b>
<b>14. Links with other policies.....</b>	<b>14</b>
<b>15. Useful Links for Educational Settings.....</b>	<b>14</b>

# Mersham Primary School Online Safety Policy

## 1. Policy Aims

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, 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

## 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 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 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 Board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

#### 3.2 The Headteacher

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

#### 3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) [and deputies] 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 ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure 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
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (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 board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, 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 Technician (Via NCS)**

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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily basis via McAfee anti-virus system.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 ensuring 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 how to report any incidents of those systems or processes failing by reporting to the Headteacher or Chair of Governors.

- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

## 3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? - [UK Safer Internet Centre](#)
- Online safety topics for parents/carers - [Childnet](#)
- Parent 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 Safer Use of Technology – See also Acceptable Use Policies.

#### 4.1.1 Classroom Use

- Mersham Primary School uses a wide range of technology. This includes access to: (desktop computers, laptops, iPads - this list is not exhaustive)
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, webcams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- All devices are password protected
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  - E.g. SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.

- We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - Early Years Foundation Stage and Key Stage 1
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
  - Key Stage 2
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

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

All schools have to teach:

- [Relationships education and health education](#) in primary schools

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

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

## **4.3 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

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The 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
- 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.

## 4.5 Vulnerable Learners

- Mersham Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Mersham Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. (this will be agreed with the SENCO and parents (where needed) on an individual basis)
- When implementing an appropriate online safety policy and curriculum Mersham Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating Parents/Carers About Online Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information shared by annual Online Safety assemblies presented by the children.. 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 and Anti-Bullying 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 are encouraged to do so, including where they are a witness rather than the victim.



The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. 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).

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

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

## 6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in our Behaviour Policy), 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 / DSL / appropriate staff member]
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Only the headteacher (or deputy headteacher in their absence) 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 headteacher/deputy headteacher in to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/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.

## 6.4 Artificial intelligence (AI)

Generative artificial intelligence (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.

Mersham 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.

Mersham Primary School will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying and Behaviour policy.

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

## 7. Acceptable use of the internet in school

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. Please read the Acceptable Use Policy for further detail. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

### 7.1 Filtering and Monitoring

This is managed and monitored by NCS using 'Netsweeper' filtering system. NCS (our IT support team) liaise directly with Broadband 4 on our behalf. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

### 7.1.1 Filtering

- Education broadband connectivity is provided through Broadband 4
- We use Netsweeper which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with NCS and Broadband 4 to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
  - Turn off monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

### 7.1.2 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - physical monitoring (supervision), monitoring internet and web access (reviewing log file information) and/or active/pro-active technology monitoring services.
- If a concern is identified via monitoring approaches we will:
  - Inform the DSL or deputy who will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

## 8. Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all but the youngest users. (Note: this should be in place for all except Early Years and Foundation Stage children and some learners with SEND)
- All users are expected to log off or lock their screens/devices if systems are unattended.

## 8.1 Password Policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- Change their passwords every season.

- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

## 8.2 Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

## 8.3 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the headteacher if they receive offensive communication, and this will be recorded on My Concern.

### 8.3.1 Staff email

The use of personal email addresses by staff for any official setting business is not permitted.

- All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents

## 9. Pupils using mobile devices in school

We understand that some of our older pupils may have permission to walk home unaccompanied. Therefore, pupils may bring mobile devices into school, but these are to be handed to the school office immediately and can be collected again at the end of the school day. are not permitted to use them during:

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 can be made up of [three random words](#), in combination with numbers and special characters if required, or generated by a password manager
- 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 by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use (please see the Acceptable Use Policy)

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager (NCS Solutions)

## 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 (Behaviour Policy, Acceptable Use Policy). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

## 12. Training

### 12.1 Staff, governors and volunteers

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, 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
- 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputies 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.

## 12.2 Pupils

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 training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 13. Monitoring arrangements

All members of staff log behaviour and safeguarding issues related to online safety using our online system, My Concern.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 14. 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
- Acceptable Use Policy
- Social Media Policy

- Anti-Bullying Policy
- Mobile and Smart Technology Policy

## 15. Useful Links for Educational Settings

### **Kent Support and Guidance for Educational Settings**

#### **Education Safeguarding Team:**

Rebecca Avery, Online Safety Officer

Ashley Assiter, Online Safety Development Officer Tel: 03000 415797

Guidance for Educational Settings:

[www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)

[www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)

[www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links)

Kent Online Safety Blog: [www.theeducationpeople.org/blog/?tags=Online+Safety&page=1](http://www.theeducationpeople.org/blog/?tags=Online+Safety&page=1)

KSCMP: [www.kscb.org.uk](http://www.kscb.org.uk)

#### **Kent Police:**

[www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

#### **Front Door:**

The Front Door can be contacted on 03000 41 11 11

Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

#### **Early Help and Preventative Services:**

[www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts](http://www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts)

#### **Other:**

Kent Public Service Network (KPSN): [www.kpsn.net](http://www.kpsn.net)

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: [www.eiskent.co.uk](http://www.eiskent.co.uk)

National Links and Resources for Educational Settings

CEOP: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) [www.ceop.police.uk](http://www.ceop.police.uk)

Childnet: [www.childnet.com](http://www.childnet.com)

ChildLine: [www.childline.org.uk](http://www.childline.org.uk)

Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)

Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)

NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)

Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)

The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)

UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)

360 Safe Self-Review tool for schools: [www.360safe.org.uk](http://www.360safe.org.uk)

#### **National Links and Resources for Parents/Carers**

Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org)

Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)

Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)