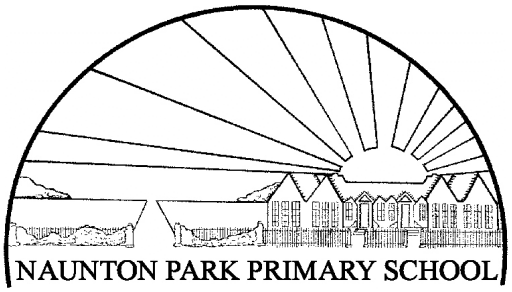

Naunton Park Primary School

Online Safety Policy (including Acceptable Use)

Last review date: Sept 2024
Next review date: Sept 2025

Approved by Governors 8.10.24

Contents

1.0 Aims

Naunton Park Primary 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.

1.1 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, antisemitism, radicalisation and extremism;
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and 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.

2.0 Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education (2024), 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

This policy 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.

3.0 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:

- 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.
- 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.
- 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).
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and regularly review their effectiveness. The Governing Body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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.
- 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. The Headteacher will liaise with the Chair of Governors and/or professionals at Gloucestershire County Council, as required, regarding any concerns about adult use of the internet or devices in school (or owned by school).

3.3 The Designated Safeguarding Lead (DSL) and Deputy (DDSL)

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 (but not limited to):

- 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 Body 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.
- Working with the Computing Lead and the ICT Manager to make sure the appropriate systems and processes are in place.

- Working with the Headteacher, Computing Lead and other staff, together with the ICT Manager and monitoring software provider 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.
- 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 and the school's Anti-bullying and Hate 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 Body.
- Undertaking annual procedural and policy reviews, which consider and reflect on the risks children and staff face.
- Undertaking additional risk assessments, when and as required, based on the needs of individual children and staff.
- 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.
- Completing the relevant induction with newly appointed staff, including governors and volunteers, relating to safe use of devices and online safety in school.
- Ensure all staff have secure access to all relevant websites as required to effectively carry out their role, including email, CPOMS and Insight.

3.4 The ICT Manager

Focus Networks provide the ICT management for Naunton Park Primary School. They are responsible for (but not limited to):

- 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 as per the contract.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- 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 dealt with appropriately in line with the school behaviour policy.
- Ensuring that the most up-to-date software and operating systems are installed on each device as required.
- Creating usernames and passwords for all staff and pupils to use when accessing school-owned devices.

3.5 All staff and volunteers

All staff, including contractors, agency staff and regular volunteers, are responsible for (but not limited to):

- 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 2) and ensuring that pupils follow the school's terms on acceptable use (appendix 1).

- 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 referring them to the DSL via CPOMS.
- Understanding that the Senior Leadership Team, ICT Manager, Computing Lead and/or DSL/DDSLs are permitted to monitor the use of school-owned devices at any time.
- Following the correct procedures directed by the ICT Manager 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 on CPOMS 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 and Anti-bullying and Hate 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'.
- Accessing only the networks, websites, software and files required to effectively carry out their individual, professional role.
- Seeking advice from the DSL and/or Headteacher if they have a concern about their own or others' use of a device or the internet.

All contractors, agency staff and volunteers are provided with a leaflet, summarising the school's child protection and safeguarding policy and procedures, including the acceptable use of devices, software and the internet.

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.
- Read correspondence sent from the school about keeping safe online and the safe use of devices.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).

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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Additional information for parents/carers and staff can be found on the school's website and in the school's newsletter.

3.7 Visitors

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

All visitors are provided with a leaflet, summarising the school's child protection and safeguarding policy and procedures, including the acceptable use of devices, software and the internet.

4.0 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study and from the guidance on relationships education, relationships and sex education (RSE) and health education. All schools must teach relationships education and health education.

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

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

Pupils in **Key Stage 2** will be taught to:

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

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

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

The safe use of social media, the internet, software and devices 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.

In addition to the statutory curriculum, further opportunities to teach children about online safety and the safe use of devices are provided, including through:

- Life Education with GHLL (Gloucestershire Healthy Living and Learning).
- Internet Safety Day.
- Children's Mental Health Week.
- Skill Zone.
- School Beat workshops.
- Anti-bullying Week.
- Safeguarding assemblies.

5.0 Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety and the safe use of devices through letters, newsletters, social media (e.g. Facebook), the school's website and other communications home. Workshops

and information events may also be offered to parents. This policy will also be shared with parents/carers. Parents are encouraged to discuss relevant matters with their child.

Online safety will also be covered during parents' evenings as necessary.

The school will let parents/carers know:

- What systems the school uses to filter and monitor the use of devices, software and the internet.
- 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 their child's class teacher.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6.0 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 one 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 and Hate 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. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including personal, social, health and economic (PSHE) education, computing lessons and extra-curricular activities 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 sends information/leaflets on cyber-bullying to parents/carers (most often via the school's newsletter) so they are aware of the signs, how to report it and how they can support children who may be affected. The school is aware the cyber-bullying affects pupils outside of school and relies on parents/carers to take appropriate action to monitor their child's activity and act upon any concerns if/as they arise. If incidents that take place out of school are brought to the attention of staff members in school, then a member of the senior leadership team and/or DSL will investigate allegations or concerns and speak directly with the parents/carers of those involved. Additional support in school may be put in place as relevant in the form of extra online safety lessons or activities led by professionals from the police or School Beat team for example.

The school's DSL and deputies monitor the use of devices and internet each week using Securus software. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy, child protection policy 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.

7.0 Examining electronic devices

Through training and regular updates to staff about policy, procedures and risks of online safety and the safe use of devices, staff are aware that they must report any concerns relating to the failure of complying to this policy. Incidents and/or concerns are reported to the DSL via CPOMS or the Headteacher verbally if relating to a member of staff. Any concern relating to the Headteacher should be reported to the Chair of Governors.

Additionally, the DSL and deputies are responsible for working directly with Focus Networks to ensure the safe use of devices, software and the internet and use Securus to directly monitor the use of these. Device use is monitored by the DSL and DDSLs weekly during safeguarding meetings.

The Headteacher, and any member of staff authorised to do so by the Headteacher, for example a member of the senior leadership team or the Computing Subject Lead, 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
- Has been used in a way that does not adhere to this policy, the staff conduct policy, the school's behaviour policy or child protection policy, 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 and/or DSL.
- Explain to the individual (staff or pupil) why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the individual's co-operation.

Authorised staff members may examine (or request that a third party, e.g. Focus Networks or Securus) 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 or erase data or files (including search history) 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 values and safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If such material is found on the device, it is up to the staff member in conjunction with the DSL and/or Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

When an image, data or file is deleted, a record of the concern will be logged on CPOMS for children or following the Low Level Concerns Policy if the concern relates to a staff member, including a visitor.

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 and/or Headteacher immediately, who will decide what to do next. The DSL and/or Headteacher will make the decision and search the device in line with the DfE's latest guidance on searching, screening 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 including computer generated imagery.

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

8.0 Acceptable use of the internet

8.1 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 (appendices 1 and 2). Visitors are expected to read and agree to the school's terms on acceptable use summarised in the visitors' leaflet provided upon arrival to the school site.

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.

The school's Wifi must not be accessed from any personal device. Staff are prohibited from sharing the password with any visitor. Spare devices are available for visitors to access the internet, which are owned and monitored by school. In exceptional circumstances, if another professional is invited into school who needs to access their work device (if unable to use a school-device) for the purpose of their visit, then the Headteacher may authorise access to the school Wifi. It will be noted on the visitors' records that the Wifi was accessed for future reference if required.

The DSL, Deputy DSL and/or Headteacher 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 and 2.

Monitoring software, Securus, is used by the DSL and deputies to monitor internet searches, visited websites and on-screen data each week. More information about examining electronic devices is explained in Section 7.0 of this policy.

8.2 Acceptable use of email systems

All staff use Office 365 for work emails. Outlook can be downloaded and used to access work email accounts. All emails sent relating to school, including and especially naming pupils, must only be sent/received via work email accounts.

Work emails can be accessed outside of school on a personal device only when:

- The device is password protected.
- The application/software used to access the email account, e.g. Outlook, is password protected.
- Emailed files are not downloaded onto the personal device.
- Notifications/alerts do not display any part of the email on the home/lock screen.

Egress Switch must be used when emailing external professionals about a child.

All pupils have a school email address created upon their admission to the school. Pupil email addresses, however, are only used if required for remote learning purposes in the case, for example, a school closure.

8.3 Acceptable use of social media

The school uses social media to communicate with parents/carers, governors and the local community. Only authorised staff are permitted to post content on the school's social media accounts and these usernames and passwords are kept securely by these authorised staff members.

Only content relating to school must be posted on the school's social media accounts. Pupils' names and images of their faces are not to be posted on any social media account, even if the pupils have photo permissions from their parent/carer.

The school's authorised users have the required technical permissions to authorise/delete comments made by others on social media posts. It is at their discretion as to whether a post should be visible or deleted on the school's social media accounts.

Staff are permitted to access their personal social media accounts in school only during break times and when not in the presence of pupils and visitors to the school. Staff must not post the names or images of any child on their personal social media account. The school's Staff Conduct Policy applies to communication and posts made by staff on their personal social media accounts. Staff are not permitted to 'follow' or become 'friends' with any pupil of the school on their social media account. Staff are expected to have their privacy settings to the highest level on any social media platform to protect their own privacy.

When carrying out online checks during the recruitment process, only the school's social media accounts are to be used. Staff members' personal accounts must not be used when completing these online checks.

8.4 Publishing content online

Section 8.3 details the content and permission for publishing on the school's social media accounts.

Staff are able to publish content on the school's website with individual usernames and passwords. They must only login using their individual account. Authorised staff have a higher level of access to the school website and they are able to delete a user's access if it is deemed necessary.

The content published on the school's website, in the Newsletter or sent via email is limited to:

- School related content;
- Images or videos of pupils who have the relevant permissions from their parent/carer and without names attached;

Forenames and photographs/videos of pupils may be used (with parental permission) if it is not possible to identify a child by their face or name.

Photographs and names of staff members are published on the school's website, newsletter and/or used in email communication unless permission has been withdrawn. To withdraw permission, a staff member should first speak to the Headteacher to better understand how and why the information is published. Their withdrawal of permission should then be made in writing to the Chair of Governors. Names and photos of staff on the website, newsletter or email are only published in the best interest of the school and for information purposes.

8.5 Acceptable use of video conferencing

Microsoft Teams, School Cloud and Zoom are used for video conferencing with parents/carers, pupils, governors and/or other professionals.

All involved in video conferencing must:

- Fully clothed.
- Inform all others around them that a meeting is taking place.
- Conduct the meeting from a private space and, where possible, wear headphones and a microphone.
- Never record a meeting without informing all attendees and receiving their permission.

To access online meetings, school staff must use their work email address.

9.0 Acceptable use of devices

9.1 Pupils using mobile devices in school

Pupils may bring mobile devices into school if their parent/carer provides written consent for them to do so and, together with the child, agrees to the safe use of the device.

When bring a personal device onto the premises, the child (and parent/carer) must agree to:

- Switch the device off before entering the school site, including before entering the playground.
- Hand the device into the school office immediately, often done via the class teacher in a wallet with devices brought into school by other children.
- Collect the device from the school office at the end of the school day.
- Keep the device switched off until the child has left the premises.

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. Individuals will not be permitted to bring their device into school if they fail to adhere to this policy following a verbal warning. This will be communicated to their parent/carer by the class teacher, DSL or Headteacher. A record of such warning and any banning of a device from the premises is logged on CPOMS.

9.2 Staff using personal devices in school

Staff, including visitors, may bring personal devices into school. They must not, however, use personal devices:

- In the company of pupils.
- During curriculum time.
- To take any photograph or video on the school premises or during any external visit.
- To access the school's Wifi.

Posters are displayed in the school's reception area to remind visitors that photographs and videos are not permitted. The leaflet given to all visitors explains the permitted use of personal devices in school.

CPOMS' Two Factor Authentication requires staff to use their personal device to generate a code that enables them to securely access CPOMS on a school device. CPOMS must not be accessed via a personal device other than to approve a secure login using the CPOMS Two Factor Authentication APP.

9.3 Pupils using school-owned devices outside of school

All pupils are expected to adhere to this policy when using a school-owned device, both in school and (if applicable) at home. All pupils have a username/password set up upon their admission to the school in order to access school laptops.

When using a school-owned laptop, pupils:

- Only use their personal login.
- Use only the software and/or websites directed by the class teacher or supervising adult.
- Report any concerning content, if seen, to an adult immediately.
- Logout of the device before switching it off.

When using a school-owned iPad or tablet, pupils:

- Use only the Apps and/or websites directed by the class teacher or supervising adult.
- Report any concerning content, if seen, to an adult immediately.
- Do not take any photographs or videos unless directed to do so by the class teacher or supervising adult.

9.4 Staff using school-owned devices outside of school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for more than ten minutes or if the staff member leaves the device unattended.
- Not sharing the device among family or friends.
- Ensuring the device is installed with anti-virus, anti-spyware software and monitoring software.
- Ensuring that the device is available for any software or operating system updates required.

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 2, or staff conduct policy.

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.

10.0 Response 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, anti-bullying and child protection. 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 Conduct Policy. 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.

11.0 Staff training, including induction

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, the newsletter 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, 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. -
- 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. They will also receive information as required, delivered by the DSL, at governor meetings.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12.0 Monitoring arrangements

Staff log behaviour and safeguarding issues relating to online safety or device misuse using CPOMS. CPOMS is regularly monitored by the DSL and Deputies. Weekly safeguarding meetings are held, in which the DSL and deputies discuss online safety and/or device use concerns that have been logged on CPOMS. Additionally, the DSL, deputies and/or members of the Senior Leadership Team use the school's monitoring software to scrutinise, and follow up if necessary, any concerns with the use of school-owned devices or internet use.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the Governing Body.

An internal review of the school's procedures will be carried out by the DSL to consider and reflect on the risks pupils and staff face online (and when using devices) and how the school's policy reduces and manages these risks. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The review also provides an opportunity for the DSL, governors and SLT to ensure the school's procedures reflect current guidance and adhere to statutory requirements.

13.0 Links with other policies

This online safety policy is linked to the school's:

- Child protection and Safeguarding policy;
- Behaviour policy;
- Staff Conduct Policy;
- Data protection policy and privacy notices;
- Complaints procedure;
- Anti-bullying and Hate Policy;
- RSE Policy.

Appendix 1 – Acceptable Use Agreement for pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Name of pupil:	
I will read and follow the rules in the Online Safety and Acceptable Use Policy. **When I use the school's ICT systems (including the internet, computers and tablets), I will:** • Always use the school's ICT systems and the internet for educational purposes only. • Only use them when a staff member is present, or with a staff member's permission. • Only use my login on school laptops and keep my usernames and passwords private. • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of a staff member or parent/carer. • Tell a known adult immediately if I find any material which might upset, distress or harm me or others. • Always log off or shut down a computer when I've finished working on it. • I will comply with the school's behaviour policy during video conferencing and remote learning activities. **I will not:** • Access any websites and applications that are not required for my work, including: social media, chat rooms and gaming sites. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any hurtful or offensive language when communicating online, including in emails. • Create, link to or post any material that could upset someone. • Log in to the school's network using someone else's details. • Take photos or videos of anyone in school unless I have permission from a staff member. • Contact a member of staff via social media or any other software without permission from them and my parent/carer and only use a school email account to contact my teacher with their permission. • Download any software or APPs unless asked to do so by an adult. **I will only bring a personal mobile device into school with written permission from my parent/carer. If I bring a personal mobile or other personal electronic device into school:** • I will turn my mobile phone off before entering the school's grounds and will take it to the school office as soon as I arrive in school. I will collect it at the end of the day and keep it switched off until I leave the school site. • I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online. I will not use it to contact any member of staff. **I agree that the school will monitor the websites I visit, my email and Teams account and the text/images I use and view. I am aware that there will be consequences if I don't follow these rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: 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 to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2 – Acceptable Use Agreement for 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 (as defined by this policy) material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms other than school accounts as an authorised user.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or applications or connect unauthorised hardware or devices to the school's network.
- Share my username/password with others or log in to the school's network using someone else's details.
- Take photographs or film pupils who do not have written permission from a parent/carer.
- 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.
- Communicate with pupils or parents/carers via social media or my personal email account.

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, including email, Microsoft Teams and my school laptop.
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 ensure that I have logged out of confidential websites and locked my computer if leaving it unattended. I will blank-out my screen if approached while working with confidential information.
I will report any cyber-bullying, device/internet misuse or any concern raised about or by a pupil that might upset, distress or harm them or others in line with this policy.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
I will always conduct video conferences in line with this policy.
I will report any activity deemed to be a safeguarding concern using CPOMS (if involving a child) or directly to the DSL/Headteacher (if involving an adult).
I will report any filtering issues to the ICT Manager immediately.
On a personal device, I will not:

- Access the school's Wifi or share the Wifi password without permission from the Headteacher or a member of SLT.
- Take photographs or film pupils under any circumstances.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Communicate with pupils or parents/carers via social media or email.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Signed (staff member/governor/volunteer/visitor):	**Date:**