Pinfold Street Primary School

*Equipping pupils with the skills and knowledge to be 'Prepared for Life'.*

# Online safety policy

Pinfold Street Primary School

| | |
|---|---|
| **Approved by:** | Governors on 20th October 2025 |
| **Last reviewed by and on:** | Toni Beech September 2025 |
| **Next review due by:** | July 2025 |

| Version | Date | Author | Summary of Changes | Approved By |
|---|---|---|---|---|
| 1.0 | Sep 2023 | Toni Beech | Initial policy creation using The Key template | Governing Body |
| 1.1 | Sep 2024 | Vicky Ashfield | Supporting pupils at risk online<br>Added filtering and monitoring<br>Add 6.4 Using AI | Governing Body |
| 1.2 | 10/10/2025 | Toni Beech | Added i-Pad monitoring<br>How we do our filtering checks | Governing Body |

# Contents



## 1. 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 harms 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) 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 that all staff receive regular 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 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 their safeguarding needs.

The governor who oversees online safety is Vera Johnston.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- 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
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

Details of the school's DSL and deputy 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 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 child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged onto CPOMs 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 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
- Providing regular reports on online safety in school to the headteacher and/or governing board

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, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly/monthly or half-termly basis depending upon the requirements

  Checks for our filtering system is completed via: TestFiltering.com: Verify your Internet is Filtered | Test Filtering

  We run a test on a staff device and a student device, we also check chromebooks, laptops and i-Pads.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring 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

This list is not intended to be exhaustive.

We use LA-ICT for support with filtering. We use Smoothwall for monitoring.

From April 2025, all school i-Pads are monitored.

### 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, and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- 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
- Following the correct procedures by e-mailing LA-ICT to request access if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

### 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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating pupils about online safety

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

The information below has been taken from the National Curriculum computing programme of study, as well as the guidance on relationships education, relationships and sex education (RSE) and health education.

**All** schools have to teach:

- Relationships education and health education in primary schools

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
- Be discerning in evaluating digital content

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

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

The safe use of social media and the internet will also be covered in other subjects where relevant and in assemblies and National Internet Safety Day.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

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 one 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 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 within lessons. An annual 'Anti-bullying Week' is held to further raise awareness.  E-safety is an important part of the Curriculum and information for parents is included in newsletters and on the School's website.

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 so that they are aware of the signs, how to report it and how they can support children who may be affected. E-safety workshops are held to raise parents' awareness of cyberbullying.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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 Bard.

The 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.

The school will treat any use of AI to bully pupils in line with our 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.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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. Smoothwall is our monitoring system and we receive weekly reports.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## 8. Pupils using mobile devices in school

Year 6 pupils may bring mobile devices into school, but must hand them to teachers and they are not permitted to use them during the school day.

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.

## 9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, 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 Verity Singleton/LA-ICT.

## 10. How the school will respond to issues of misuse

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

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

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

## 11. Training

All new staff members will receive training, as part of their induction, on 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, 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 the risks up
- 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 deputy/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. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report can be printed from CPOMs.

This policy will be reviewed every year by the Online Safety lead. 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.

## 13. 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
- ICT and internet acceptable use policy
- Relationships and Sexual Health Education

## Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Pinfold Street Primary School

### KS1 Acceptable Use of Technology Agreement

**My name is**_____ **Class** _____

I will only use the internet when an adult is with me.

I will keep my personal information and passwords safe.

I will only send messages that are polite and friendly.


I can ask an adult if I need to learn more about staying safe online.

I will help my friends to stay safe online.

I know my teachers can see what I am doing on school technology, even when I use it at home.

I always tell an adult if something online makes me feel upset, scared or worried.

I will only click on links and buttons when I know what they do. If I'm not sure, I will ask an adult.

If I see something online that makes me upset, scared or worried I can talk to:

at home _____

at school _____

I have read and talked about these rules with my teacher, parents or carers.

# Parent Acceptable Use of Technology Agreement

- I know my child will be provided with internet access in order to access the curriculum and prepare them for modern life.
- I understand the schools Acceptable Use Agreement relates to all school technology onsite and at home.
- I understand my child needs a safe and appropriate place to access online learning.
- I am aware all school technology is appropriately filtered and monitored to ensure my child is safe when online.
- I am aware my child will receive online safety education to enable them to use the internet safely both in and out of school.
- I have discussed the content of this policy with my child.
- I will support online safety by ensuring I use appropriate parental controls and discuss online safety while using home technology.
- I know I can receive support from school regarding online safety by emailing info@pinfold-st.walsall.sch.uk
- I will model safe and positive online behaviour for my child.
- I understand that a partnership approach to online safety is required.

Signed _____

# Appendix 2: KS2 acceptable use agreement

Pinfold Street Primary School

## KS2 Acceptable Use of Technology Agreement

**I understand that the school Acceptable Use of Technology Agreement will help me stay safe and happy online at home and at school.**

**Staying safe**

I will:
behave online the same way as I behave in the classroom.
only send message which are polite and friendly.
only post pictures or videos if I have permission and they are safe and appropriate.
only talk with and open messages from people I know.
only click links if I know they are safe.
not trust that people online are always who they say they are. If someone suggests meeting up I will always tell an adult.

**Learning**

I will:
always ask permission from an adult before using the internet.
only use websites and search engines my teacher has chosen.
only use school devices for schoolwork unless I have permission to do otherwise.
follow the school technology agreement when learning online at home.

**Trust**

I will:
understand that not everything and everyone online is honest or truthful.
check content through various sources, such as other websites, books or a trusted adult.
always credit the person or source that created and work, images or text I use.

**Responsibility**

I will:
keep my personal information safe and private online.
keep my passwords safe and not share them.
not access or change other people's files or information.
only change the settings on a device if an adult has allowed me to.

**Tell**

I will:
tell or show an adult if I see anything online that makes me feel worried or upset.
report it to an adult if I am aware of ANYONE being unsafe with technology.
understand that it is not my fault if I see something inappropriate online and will always tell an adult.

**Understand**

I will:
understand that the school filter is there to protect me and I will not try and bypass it.
understand that school devices (including ones used at home) are monitored to help keep me safe.
visit www.thinkyouknow.co.uk or www.childline.org.uk if I need to know more about staying safe online.

# Parent Acceptable Use of Technology Agreement

- I know my child will be provided with internet access in order to access the curriculum and prepare them for modern life.
- I understand the schools Acceptable Use Agreement relates to all school technology onsite and at home.
- I understand my child needs a safe and appropriate place to access online learning.
- I am aware all school technology is appropriately filtered and monitored to ensure my child is safe when online.
- I am aware my child will receive online safety education to enable them to use the internet safely both in and out of school.
- I have discussed the content of this policy with my child.
- I will support online safety by ensuring I use appropriate parental controls and discuss online safety while using home technology.
- I know I can receive support from school regarding online safety by emailing info@pinfold-st.walsall.sch.uk
- I will model safe and positive online behaviour for my child.
- I understand that a partnership approach to online safety is required.

Signed _____

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

**1. Purpose**
This policy sets out the expectations for the acceptable use of digital technology and school networks by all staff members at Pinfold Street Primary School. It aims to protect staff, pupils, and the school by ensuring responsible, safe and secure use of technology.

**2. Scope**
This policy applies to all staff, including permanent, temporary, supply and volunteer staff who access the school's digital systems, networks, and devices.

**3. General Principles**
- Staff must use school technology and digital resources primarily for educational and professional purposes.
- All users are expected to act responsibly, ethically, and legally when using digital technology.
- Staff should respect the privacy and data protection rights of pupils, colleagues, and the school.

**4. Acceptable Use of School Devices**
Staff must:

- Use strong, unique passwords and change them regularly.
- Keep login details confidential and not share accounts.
- Lock or log out of devices when unattended.
- Use multi-factor authentication where available.
- Access only the systems and data necessary for their role.
- Report any cyber security incidents or suspicious activity promptly to IT support or the designated digital lead.
- Follow the school's safeguarding policies, especially regarding online safety with pupils.
- Use school-approved software and platforms for communication and data storage.
- Ensure that any personal use of school technology is minimal, does not interfere with professional duties, and complies with this policy.
- Ensure safe keeping of school devices when taken out of school.

**5. Unacceptable Use of School Devices**
Staff must not:

- Access, create, or distribute inappropriate or offensive material.
- Use school technology for personal financial gain or political activities.
- Install unauthorised software or hardware on school devices.
- Bypass security controls or attempt to gain unauthorised access to systems or data.
- Share sensitive or personal data outside the school without proper authorisation.
- Use removable storage devices (e.g., USB drives) without prior approval and scanning for malware.
- Use social media or communication tools to engage in behaviour that could damage the school's reputation or breach confidentiality.

**6. Use of emails**
- The school provides each member of staff with an email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

- Staff must take care with the content of all email messages, as incorrect or **improper statements** can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as **potentially retrievable**.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the Headteacher and SBM immediately and follow our data breach procedure.

**7. Use of mobile devices**

- Personal use of mobile phones should be limited to breaks and away from pupil areas to maintain professionalism and focus (unless there is a specific need, which has been agreed by the HT).
- Mobile phones should not be taken into the Early Years.
- No photographs of pupils should be taken on personal phones
- Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4 and 5.

**6. Data Protection and Confidentiality**

Staff must comply with data protection legislation and school policies regarding the handling, storage, and sharing of personal data. Any data breaches must be reported immediately to the Data Protection Officer (DPO).

**7. Training and Awareness**

Staff will receive regular training on cyber security, data protection, and online safety as part of their professional development. It is the responsibility of each staff member to stay informed about cyber risks and best practices.

**8. Monitoring and Compliance**

The school reserves the right to monitor the use of its technology and networks to ensure compliance with this policy. Breaches may result in disciplinary action, including termination of employment.

**9. Reporting Concerns**

Any misuse of mobile phones/devices by staff or pupils should be reported immediately according to the school's safeguarding procedures – see whistleblowing policy.

**10. Agreement**

All staff must read, understand, and sign this Acceptable Use Agreement at the start of each academic year or when they join the school.

**Signed: _____Name: _____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? | |
| 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? | |