ONLINE SAFETY POLICY

(INCLUDING MOBILE PHONE AND TECHNOLOGIES POLICY)

Last Reviewed – August 2023
Next Review – August 2024
Review Information – Annually or following a change in legislation

Read and signed by

Richard White, Chair of Managing Council **Date:**

A copy of this policy is published on the school website for parents.

REVIEW JOURNAL

Version	Approved By	Revision Date	Description of change/review	Author
V3	HM	September 2023	Whole policy review with reference to key safeguarding legislation including KCSiE 2023	HM/LTE/CW
V2	HM	August 2022	Updates in relation to KCSiE 2022	HM/LTE
V1	HM	October 2021	Reviewed by relevant staff. Check through of corresponding forms and paperwork.	HM/LTE

DOCUMENTS & GUIDANCE USED IN REVIEW PROCESS

Document/Guidance	Date
KCSiE 2021	Oct 21
ISI Commentary 2021 – 2022	Oct 21
Teaching Online Safety in Schools 2019	Oct 21
DfE Relationships Education, Relationships & Sex Education (RSE) and Health Education	Oct 21
Safer children in a digital world – Professor Tanya Byron, 2008	Oct 21
Sexual Violence and Sexual Harassment Between Children in Schools and Colleges	Sept 21
KCSiE 2022	Aug 22
DfE Education in a Connected World	Aug 22
SWGfL Online Safety: swgfl.org.uk	Aug 22
DfE Harmful online challenges and online hoaxes	Aug 22
KCSiE 2023	Sept 23
Protecting Children from Radicalisation	Sept 23
DfE Preventing and Tackling Bullying	Sept 23
Cyber-bullying: Advice for headteachers and staff, Nov 2014	Sept 23

TO BE READ IN CONJUNCTION WITH:

Document/Guidance
Child Protection Policy & Procedures
Behaviour, Rewards & Exclusions Policy

Anti-Bullying Policy
Staff disciplinary procedures
Data protection policy and privacy notices
Complaints procedure
Acceptable use policies (see appendices)
Visitor and Safeguarding Information leaflet
EYFS Policy

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 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, 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. LEGISLATION & 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.

3. ROLES AND RESPONSIBILITIES

3.1 The Managing Council (ManCo)

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

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

The ManCo 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 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.

The ManCo member who oversees online safety is Robert Ackland

All ManCo members 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

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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ManCo 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 ICT provider to make sure the appropriate systems and processes are in place
- Working with the ICT provider 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
- 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 ManCo
- 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
- 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.

3.4 The ICT provider (Aztek)

The ICT provider 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are notified to the DSL so they can be logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and 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 filling in a Cause for Concern Form
- Following the correct procedures by asking the School Business Manager and DSL 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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

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 text below is taken from the National Curriculum computing programmes of study.

It is also taken from 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
- Relationships and sex education and health education in secondary schools

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

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

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

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

The safe use of social media and the internet will also be covered in other subjects, eg Life Skills, Computing and cross-curricular where relevant.

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 via our home learning website and weekly newsletter. 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:

- That the school uses Sophos to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

6. CYBER-BULLYING

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and 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. Life Skills teachers and Form Teachers will discuss cyber-bullying with year groups.

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 (which we call Life Skills), and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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

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

6.3 Examining electronic devices

The headteacher, and in her absence, the deputy head, 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 (if she is off site)
- 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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to head teacher or deputy 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 Bard.

Polwhele House 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.

Polwhele House School will treat any use of AI to bully pupils in line with our anti-bullying 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/carers, staff, volunteers and ManCo members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet 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.

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

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but must sign them into the School Office on arrival and retrieve them at the end of the school day.

Any breach of this agreement by a pupil may trigger disciplinary action in line with the Behaviour, Rewards and Exclusions 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 or school email accounts among family or friends
- Installing anti-virus and anti-spyware software as directed by SLT
- 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, 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 Aztek (IT provider), copying in the School Business Manager.

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 and internet acceptable use. 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 the 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.

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 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 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.

ManCo members 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 manages reports recorded on Every around behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the head teacher. At every review, the policy will be shared with the ManCo. 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
- Anti-bullying policy
- EYFS policy
- Acceptable Use Policies

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

Polwhele House
GROWING CORNWALL'S FUTURE

PRE-PREP ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

READY	RESPECTFUL	SAFE

Name of pupil:

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

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

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

Signed (pupil):	**Date:**

Parent/carer 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

PREP ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

READY	RESPECTFUL	SAFE

Name of pupil:

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

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

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

I will not:

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

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

- I will sign it into the School Office before the start of the school day.

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

Signed (pupil):	**Date:**

<table>
<tr><td colspan="2"><b>Parent/carer’s agreement:</b> 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.</td></tr>
<tr><td><b>Signed (parent/carer):</b></td><td><b>Date:</b></td></tr>
</table>

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, MANCO MEMBERS, VOLUNTEERS AND VISITORS

READY	RESPECTFUL	SAFE

Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Mobile Phone and Technologies Policy

MOBILE PHONES AND TECHNOLOGIES POLICY

Last Reviewed – November 2023
Next Review – November 2024
Review Information – Annually or following a change in legislation

Read and signed by

Richard White, Chair of Managing Council **Date:**

REVIEW JOURNAL

Version	Approved By	Approved ManCo By	Revision Date	Description of change	Author
V1	HM		Nov 2023		HM/LTE

DOCUMENTS & GUIDANCE USED IN REVIEW PROCESS

Document/Guidance	Date
Statutory Framework for the Early Years Foundation Stage, 2023	November 2023
Keeping Children Safe in Education, 2023	November 2023
Working Together to Safeguard Children, 2018	November 2023

TO BE READ IN CONJUNCTION WITH:

Document/Guidance
Child Protection Policy & Procedures
EYFS Policy
Online Safety Policy including Acceptable Use Policies
Staff Handbook
Anti-Bullying Policy

CONTENTS

1. INTRODUCTION AND AIMS

At Polwhele House we recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents/carers and staff, as well as the wider school community.

Our policy aims to:

- Promote, and set an example for, safe and responsible phone use
- Set clear guidelines for the use of mobile phones for pupils, staff, parents/carers and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

2. ROLES AND RESPONSIBILITIES

2.1 Staff

All staff (including teachers, support staff and supply staff) are responsible for enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The Head is responsible for monitoring the policy on an annual basis, reviewing it, and holding staff and pupils accountable for its implementation.

2.2 Governors

The Managing Council will review this policy annually following the Head's review.

3. USE OF MOBILE PHONES BY STAFF, INCLUDING IN EYFS

3.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number 01872 273011 as a point of emergency contact.

3.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Bard).

Please see the Data Protection Policy and Acceptable Use Policies.

3.3 Safeguarding

Staff must refrain from giving their personal contact details to parents/carers or pupils, including connecting through social media, personal emails addresses and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.

See the Acceptable Use Policies and Online Safety Policy.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

3.4 Safeguarding in the EYFS

As per the statutory expectations set in the Early Years Foundation Stage Framework, all staff working in the EYFS do not use their mobile phone when the children are present and are directed to leave their phone in the agreed designated area at all times. These can only be accessed on a designated break and this is away from children. Photographs must not be taken of any EYFS child on any personal phones or any other personal storage device. Only school-owned devices can be used to take photos or videos. Staff who bring personal mobile phones into the setting must ensure that there are no inappropriate or illegal content on them.

All members of staff should remain vigilant and report any concerns to the designated DSL. Parents and staff are informed of the complaints procedure and Child Protection Policy and staff are made aware of the whistleblowing procedure.

3.5 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

See Educational Visits and Trips Policy.

In agreement with the Head, staff may use personal mobile phones when working in remote locations and when supervising residential visits or school trips. Risk assessment will include mobile phone use and guides staff to only call parents using the 3CX system or dialling 141 before entering a phone number.

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil

3.6 Sanctions

Staff that fail to adhere to this policy may face disciplinary action.

See the school's staff Code of Conduct and staff disciplinary policy for more information.

4. USE OF MOBILE PHONES BY PUPILS

Pupils may bring mobile devices into school, but must sign them into the School Office on arrival and retrieve them at the end of the school day.

Any breach of this agreement by a pupil may trigger disciplinary action in line with the Behaviour, Rewards and Exclusions policy, which may result in the confiscation of their device.

The Head has the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation. The DfE guidance allows the school to search a pupil's phone if there is reason to believe the phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury. If a member of staff, parent/carer has concerns about files on a pupil's phone they should report to the Head.   Please see 6.3 of the Online Safety Policy.

5. USE OF MOBILE PHONES BY PARENTS/CARERS, VOLUNTEERS AND VISITORS

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at the Office or attend a public event at school. All visitors, including the Managing Council will be asked to read, agree and sign the relevant Acceptable Use Policy.

Parents/carers or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents/carers
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents/carers or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in section 4 above.

Parents/carers must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day.

6. LOSS, THEFT OR DAMAGE

Pupils bringing phones to school must ensure that phones are appropriately labelled and are stored in the Office during their school day, including after school clubs and any wraparound care sessions.

Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions. Staff must also secure their personal phones, as well as any work phone provided to them. Failure by staff to do so could result in data breaches.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Signs communicating this disclaimer to pupils, parents/carers and visitors are displayed in the School Office and any trip permission forms.

If a pupil's phone is confiscated it will be stored in the School Office in the lockable filing cabinet to prevent loss, theft or damage.

Lost phones should be handed in to the Office. The school will then attempt to contact the owner, if known.

7. MONITORING AND REVIEW

The school is committed to ensuring that this policy has a positive impact of pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

- Feedback from parents/carers and pupils
- Feedback from teachers
- Records of behaviour and safeguarding incidents
- Relevant advice from the Department for Education, the local authority or other relevant organisations

---

Created: September 2023
Reviewed: November 2023
Review date: Annually or following a change in legislation

Appendix 5 : Permission form allowing a pupil to bring their phone to school

PUPIL MOBILE PHONE PERMISSION FORM

PUPIL DETAILS	
PUPIL NAME	
YEAR GROUP	
PARENT/CARER NAME	

The school has agreed to allow ……………………………………………………………. to bring their mobile phone to school because they:

- Travel to and from school alone
- Are a young carer
- Are attending a school trip or residential where use of mobile phones will be allowed
- Need the phone for an educational activity during class time
- Attend before or after-school where a mobile phone is required for the activity, or to contact parents/carers

Pupils who bring a mobile phone to school must abide by the school's policy on the use of mobile phones, and its Acceptable Use Policy.

The school reserves the right revoke permission if pupils don't abide by the policy.

PUPIL SIGNATURE	
PARENT/CARER SIGNATURE	

FOR SCHOOL USE ONLY	
AUTHORISED BY:	
DATE	

Appendix 6: Mobile phone information for visitors

Use of mobile phones in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present.
- Do not take photos or recordings of pupils or staff
- Do not use your phone in lessons, or when working with pupils

No mobile phones are permitted in the Early Years Foundation Stage.

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

This statement is shared with visitors via the Visitor and Safeguarding Information leaflet given to them on arrival at the school.