Pownall Hall School

E-Safety and Acceptable Use Policy

1. Introduction

IT, digital and mobile technology resources are regarded as essential to support learning, teaching and personal and social development. They form part of an essential life skill. When using technology with young children and adults in their setting, professionals need to ensure that the resource is used safely and responsibly. This policy sets out some guidelines for all staff to use. It will be reviewed annually and made available on the Pownall Hall School website, with the salient points also included within the main body of the Child Protection and Safeguarding Policy.

We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We recognise that children need to be safeguarded from potentially harmful and inappropriate online material and the school's role within this. To address this, our school strives to:

- Have clear procedures in place to ensure the online safety of all staff and students
- Educate the school community in the safe and responsible use of online technology
- Set clear expectations for the use of online technology, including mobile phones

Our approach to online safety is framed by four main areas of risk:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. The Designated Safeguarding Lead

The Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. It is the responsibility of the DSL to liaise with staff, including teachers, learning support staff and IT support staff, on matters of safety and safeguarding and welfare, including online and digital safety and when deciding upon a referral to relevant agencies.

3. Why is internet use important?

The internet can be used to support learning as well as for social and personal development activities. It can motivate, engage and develop self esteem, confidence and as a tool for the development of social capital. It is regarded as a necessary tool, in settings, for practitioners and children.

- Internet access is an entitlement for children and young people who show a responsible and age appropriate approach to its use
- The internet is an essential element for education, business and social interaction.

4. How the internet is used

Internet access for children and young people will be designed for educational aspects of social and developmental use and will include age appropriate filtering. Guidance about appropriate Internet use will be part of the support for children and young people. All practitioners should guide children and young people in online activities that will support their developmental and learning outcomes.

5. Internet Access

All staff with access to the internet must agree to sign the induction form to confirm they have read and understood the Acceptable Use Policy before being permitted to use any of the digital or electronic resources at the School as mentioned in this policy.

All IT equipment is property of the school, therefore users are not permitted to make any physical alteration, either internally or externally, to the School's computer or network hardware. If extensive damage is caused due to software installed without permission, users may be held personally liable for rectifying the damage.

For younger users, access to the internet will be closely supervised by an adult allowing access to specific and agreed sites only. Older children and young people will be provided with wider access and greater autonomy in line with their age and maturity of use.

Communication will be made via form teachers or, where necessary, individual subject teachers, to explain when and how children are expected to use the internet safely at home for homework tasks, for example via recognised password-protected learning platforms such as ActiveLearn or MyMaths. Where children are asked to conduct research using the internet, guidance will be provided in terms of suitable websites and such tasks will be posted on Google Classroom to ensure parents are able to access instructions.

6. Filtering, monitoring and security

The Head, as the senior member of staff, and the DSL, in conjunction and consultation with the Pownall IT consultancy team (Hi-Impact Consultancy) and the safeguarding governor, Mrs A Simmonds, will manage the permitting and banning of additional web sites identified by Pownall Hall School.

If practitioners or children and young people discover unsuitable sites, the URL (address) and content must be reported to Hi Impact Consultancy either through DSL, via the Head, or directly to Hi Impact.

The Headmaster, DSL and the Safeguarding Committee including the safeguarding governor, Mrs A Simmonds, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the setting or organisation believes is illegal must be referred to the Internet Watch Foundation https://www.iwf.org.uk/report/ if and where appropriate.

Pownall Hall School uses a Safe Search filter system called 'Surf Protect' and is monitored by Hi-Impact as a filtering and monitoring system. This filters and monitors for harmful or inappropriate content. This covers our school network and the following devices: class set of Chromebooks; class set of iPads; staff laptops.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and Deputy DSLs monitor the effectiveness of this system through weekly reviews of reports sent to the Headmaster and DSL. In the event of something serious being detected, the Headmaster would be alerted immediately via email.

The school takes care not to 'over block' content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty. The filtering/monitoring arrangements are directly informed by the school's Prevent Duty risk assessment.

Staff receive regular training on the filtering and monitoring systems and staff are aware that these systems are in place.

The DfE has published filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring systems and least annually
- block harmful and inappropriate content without unreasonable impact on teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

We at Pownall Hall have done the following in relation to this: clarified the role of the DSL and the wider SLT in regularly overseeing weekly filtering and monitoring reports from Hi-Impact; reviewed our filtering and monitoring provision with a view to doing so annually, prior to the start of the academic year; ensured that harmful and inappropriate content is blocked without impairing the effective teaching of online safety; familiarised the wider school community with our filtering and monitoring systems.

When the filtering and monitoring system detects concerning usage, these are recorded in the form of weekly reports sent to the Headmaster by Hi-Impact, and appropriate action, including a referral to children's social care, is taken when necessary.

For more information on filtering and monitoring, parents and carers can contact the Headmaster, the DSL or the Safeguarding Governor.

The school has an appropriate level of security protection which is reviewed periodically to keep up with evolving cyber-crime technologies.

7. Risk Management

In line with other media such as magazines, books and DVDs, some material available via the internet is unsuitable for children and young people. Staff at Pownall Hall School will take all reasonable precautions to ensure that users access only appropriate material.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

The e-safety lead for Pownall Hall (Hi-Impact Consultancy in conjunction with the Head) will have an awareness of current e-safety advice and will embed this within the work with children and young people.

The Head and Safeguarding Committee will ensure that the Internet policy is implemented and compliance with the policy monitored.

Children will receive regular eSafety lessons as an embedded part of the IT curriculum. They will be made aware of the details within this policy.

These lessons will be carefully and sensitively tailored to meet the needs of all pupils, including those with SEND and any children who are known to be victims of abuse.

We recognise that children with SEND face additional risks, for example from bullying, grooming and radicalisation, and these children will be carefully supported to ensure they remain safe online..

8. Managing Content

If an unsuitable site is discovered, the URL (address) and content will be reported to Hi Impact Consultancy.

If appropriate, specific activities will be included within the work that Pownall Hall undertakes, to allow all children and young people to develop their media literacy skills

8.1 How should website content be managed?

- Written permission from parents or carers will be obtained before photographs of children and young people under the age of 16 are published on the settings' web site.
- Website photographs that include children and young people will be selected carefully and will not enable individuals to be clearly identified.
- Full names of children and young people should not be used anywhere on the website, first names will only be used in association with photographs.
- Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the children and young people, under the age of 16 to be identified.
- The Head will take overall editorial responsibility and ensure that content is accurate and appropriate.

9. Communication

9.1 Managing email

- The staff at Pownall Hall School will promote safe use of e-communications to other practitioners, professionals, parents/carers, children and young people.
- Children and young people should immediately report to an adult if they receive offensive emails.
- Children and young people should not reveal any details of themselves to people they do not know, such as an address or telephone number, or arrange to meet anyone.
- The staff at Pownall Hall School will use e-communications with the children and young people as it is part of the work for this group, using approved email addresses and Google Accounts.
- Younger children will not be provided with individual accounts for email. Any children who wish to set up an account whilst in our care will require written consent from their parent/carer.
- Young people should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of appropriate conduct and may be classed as bullying.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on headed paper.

9.2 On-line communications and social networking

In general, the use of online chat will not be permitted other than as part of an online learning environment i.e. Pownall's Google platform.

Underage children and young people will not be allowed access to social networking sites. The minimum age limit for accessing social networking sites is usually 12, but the staff at Pownall Hall School will need to check the terms and conditions of use for the individual site.

Social networking sites may be allowed for specific purposes, e.g. teaching e-safety.

Staff members have a responsibility to protect the reputation of the School, staff and pupils at all times. This includes extending their professionalism to social networking sites. Users ensure they do not knowingly cause annoyance, inconvenience or needless anxiety to others via social networks.

9.3 Mobile technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before its use within the school is allowed, e.g. wifi enabled notebooks.

Personal mobile phones and any electronic devices with imaging and sharing capabilities, not just mobile phones and cameras (as detailed in the EYFS Statutory Framework as issued by the DfE in January 2024), are not permitted in any form in EYFS at Pownall Hall.

From Form 1 upwards, staff are not permitted to use personal mobile phones or electronic devices with imaging and sharing capabilities in the presence of children, except in the case of emergencies (for example, a first aid situation or on a school trip). Staff mobile phones should be stored securely out of sight of children, for example in bags, cupboards or lockers when not in use.

Children are not permitted to bring mobile phones into school and any wearable devices such as fitness trackers are only acceptable if they do not have internet access, messaging or imaging/ sharing capabilities. If children require mobile phones for security or safeguarding purposes at the end of the school day (for example, because they are staying at the house of a different parent, family member or friend), they should hand in the device at Reception at the start of the school day and collect it again before departing school. Any such children then attending clubs will hand the device to the member of staff taking the club and collect it again at the end of the session.

It is recognised that many children have access to unlimited and unrestricted access to the internet via mobile phone networks (ie:3G, 4G and 5G). This access means that some children, whilst at school:

- sexually harass
- bully
- control others via their media and smart technology
- share indecent images
- view items with harmful content.

Staff should only use school iPads or mobile phones when taking any photographs or videos of children. On the rare occasion that this may not be possible, such as on a residential trip or when a school device is not working or has run out of battery and communication with parents is deemed essential, a personal mobile phone or iPad may be used. In these cases, images must be transferred to the school's secure Drive as soon as possible and deleted from the relevant device.

Personal mobile phones are not allowed to be used on school premises and are stored securely in a bag/cupboard/locker.

See Safeguarding and Taking Photo policies for more details.

10.Introduction to young children

- Rules and rights for Internet access will be posted in all areas where computers are used
- Support for responsible and safe use should precede Internet access
- Children and young people must be informed that Internet use is monitored
- The teaching of e-safety will be part of the provision for all children and young people. It will include key messages that are age and maturity appropriate, such as keeping personal information safe, dealing with cyberbullying, knowing who to tell if there is inappropriate content/contact on-line.
- Children will be made aware of the e-safety policy and the importance of e-safety.

11.Families, carers, childminders, setting managers and e-safety

- Adults' attention should be drawn to the e-safety policy.
- Regular information should be provided to parents and carers about how to ensure they can work with the school to ensure resources are used appropriately.
- A partnership approach with parents and carers should be encouraged. This could include awareness-raising meetings, newsletters and hands-on sessions and suggestions for safe internet use at home.
- Advice on filtering systems, educational and leisure activities that include responsible use of the internet should be made available to parents.
- Interested parents should be referred to organisations such as CEOP, Childnet International, Parents Online and NCH Action for Children.

12.Consulting with practitioners and their inclusion in the e-safety policy

- All practitioners should be consulted about the contents of this policy to ensure that the use of the internet and mobile technologies supports their work with children and young people in a safe environment
- All practitioners should be required to see and sign the policy for responsible email, network and internet use as part of their induction
- The consequences for internet and mobile phone/PDA/technology misuse should be clear so that all adults are confident to apply this should the situation arise (e.g. supervised access, withdrawal of access)

13. How will complaints be handled?

- Responsibility for handling incidents will be delegated to the Headmaster.
- Any complaint about practitioner misuse must be referred to the Headmaster.
- Parents and children and young people will need to work in partnership with practitioners to resolve issues should they arise
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
- Interview/counselling by a designated senior practitioner

- Informing parents or carers
- Removal of internet or computer access for an identified proportional amount of time
- Supervised access.

14. References to other policies/ agencies:

- Please see the Child Protection and Safeguarding Policy for additional clarification and relevant information, including the school's commitment to the Prevent Duty..
- Please also refer to the Behaviour Policy, Staff Code of Conduct (including acceptable use of technology therein), KCSIE 2025 and Working Together to Safeguard Children 2023.

MONITORING AND REVIEW

The Headmaster and the Safeguarding Committee will monitor this policy and review it every year or before - if procedures need to be or can be improved.

Presented to Governors for approval **September 2025**

Signed:

Mrs Eileen MacAulay, Chair of Governors *September 2025*

Revision Log

Date	Changes Made	Version No
Nov 2018	Creation of Policy	V1
Nov 2019	Reviewed and updated	V2
Nov 2020	Reviewed and updated	V3
Nov 2021	Reviewed and updated	V4
Nov 2022	Reviewed and updated	V5
Sept 2023	Reviewed and Updated	V6
Sept 2024	Reviewed and Updated	V7
Sept 2025	Reviewed: noted that children will be made aware of the contents of the policy; acknowledge children have access to external devices / internet	V8

Next Review: Sept 2026

Useful Contacts

- CEOP (Child Exploitation and Online Protection Centre) - www.ceop.org.uk
- Childnet International - http://www.childnet-int.org
- PIN – Parents Information Network - http://www.pin.org.uk
- Parents Online - http://www.parents-online.net
- NCH Action for Children - http://www.actionforchildren.org.uk
- IWF – the Internet Watch Foundation - http://www.iwf.org.uk
- Think U Know for Parents - www.thinkuknow.co.uk/parents

Appendix 1

Pupils' Responsible internet use Policy

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using a computer and the internet
- If I have an 'individual login' this is the one I will use, no-one else's, which I will keep secret
- I will only open or delete my own files
- I understand that I must not bring in and use software or files without permission
- I will only email and open attachments from people I know, or have been approved
- The messages I send will be polite and sensible
- I understand that I must never give my home address or phone number to people I do not know, or to post on a social networking site
- I will not arrange to meet people that I do not know face-to-face
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a trusted adult immediately
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers

Pownall Hall School may exercise its right to monitor the use of its computer systems, including access to web-sites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Name:

Signature:

Date:

Appendix 2

Laptop/Chromebook policy for practitioners at Pownall Hall School

- The laptop is allocated to staff and is their responsibility. If another member of the team borrows it, the responsibility still stays with the individual allocated. Only Pownall Hall staff and children within the setting should use the laptop
- All laptops storing sensitive information should have software to encrypt the data
- All laptops storing sensitive information should have password protected screen savers that will appear after two minutes
- Any unnecessary data should be deleted from the setting laptop immediately
- When in the setting and not being used, the laptop should be switched off and kept secure
- Whenever possible, the laptop should not be left in an unattended car. If there is a need to do so it should be locked in the boot
- Practitioners may load their own software onto the laptop but it must be fully licensed, age appropriate and with authorisation from the Headmaster
- If any removable media is used then it should be checked to ensure it is free from any viruses and should be saved on an encrypted memory stick
- It will be the responsibility of the setting manager to ensure virus protection software that has been installed on the laptop is kept up to date
- Practitioners should not attempt to significantly alter the computer settings without express authorisation from the setting manager
- Children and young people must never use the laptop without adult supervision and knowledge
- The laptop would be covered by normal household insurance whilst away from the premises. If not it should be kept in the setting and stored securely at all times when not in use.

Name:
Signature:
Date:

Appendix 3

Responsible e-mail, network and internet use for the staff of Pownall Hall School

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
   - Access offensive websites or download offensive material
   - Make personal use of the internet or email unless agreed by the setting manager
   - Copy information from the internet that is copyright or without the owner's permission or acknowledging copyright as appropriate
   - Place inappropriate material onto the internet
   - Communicate information that could be considered to be offensive or otherwise inappropriate
   - Disregard my responsibilities for security and confidentiality
   - Download files that will adversely affect the security of the laptop and network.
   - Access the files of others or attempt to alter the computer settings

2. I will act on-line as I would offline, in accordance with Pownall Hall School code of conduct

3. I will only access the system with my own name and registered password, which I will keep secret and safe

4. I will always log off the system when I have finished working

5. I understand that Pownall Hall School may, in line with policy, check my computer files and emails and may monitor the internet sites I visit.

6. I will not open email attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the setting manager

7. All joke emails are potentially damaging and undesirable and therefore should not be used

8. I will report immediately any unpleasant material or messages sent to me

9. I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material

10. Equipment belonging to Pownall Hall School will not be used for personal financial gain, gambling, political purposes or advertising and is forbidden.

11. I understand that if I do not adhere to these rules, my network access will be suspended immediately, the laptop removed and that other disciplinary consequences may follow.

All staff complete the induction document, see Induction of New Staff Policy, to confirm they have read and understood this policy

Appendix 4
WhatsApp and Parent Messenger – School Community Advice

The use of WhatsApp and other forms of digital messenger has increasingly become an integral part of how we communicate within the various school communities. It has made communication faster and easier than ever before and is an excellent, low-cost way to share news and events.

Usage
In line with the General Data Protection Regulations, Safeguarding legislation and to ensure the communications posted are appropriate, the School has created some guidelines for usage in relation to PHS events, pupils, parents and the wider school community.

- Only post information that you would be happy to present in any public forum.
- Share only relevant, meaningful information. A WhatsApp group with too many posts may become ineffective. Information may be missed and/or parents may opt out if the volume of messages becomes overwhelming.
- Please share photos privately. No images of children should be posted on 'Year' WhatsApp groups. A number of parents have opted out of their children being photographed and subsequently published. It is the duty of everyone to be considerate to individual preferences.
- Avoid using groups to discuss academic or school policy concerns. These should be discussed directly with the School via your child's class teacher or subject teacher in the first instance.
- Do not use it as a sales tool for your personal business.
- Do not post photographs and names of any member of staff.
- Please private message other users regarding personal events rather than replying to the group.
- Do encourage others to use WhatsApp appropriately.

Recommendations
You are personally responsible for the content you publish. Please be mindful that what you publish will be public for a long time and that you should aim to protect your privacy and that of others. Remember there is no such thing as a 'private' social media site, comments can be forwarded or copied.

The Parents' Association has been asked to utilise other forms of communication such as email for parents who have opted out of your Year WhatsApp group. Should you think that you are missing information, please do not hesitate to contact a member of the Parent's Association to ensure key messages get to you.