**Early Years Assessment Centre**
Eastmoor Road
Eastmoor
WF1 3SQ

**Forest Wood Centre**
Painthorpe Lane
Crigglestone
WF4 3HW

**Pinderfields Hospital PRU**
**01924 298351**

**Hospital tuition**
Children's Ward
Pinderfields
Hospital
Wakefield WF1 4DG
01924 541947

**Limes Centre**
Long Causeway
Stanley
WF3 4JB

**Spinney Centre**
Common Road
South Kirkby
WF9 3EA

**Thornes Centre**
Lawefield Lane
Wakefield
WF2 8ST

**Woodlands Centre**
College Grove
Castleford
WF10 5NS

**Wrenthorpe Centre**
Imperial Avenue
Wrenthorpe
WF2 0LW

# Online Safety Policy

2025-26

Chair of Management Committee
Signed

**MISSION STATEMENT**

At Pinderfields Hospital PRU we will:

- Encourage honesty, respect and trust
- Exercise discipline and self-control
- Feel safe, secure and happy in the school environment
- Develop our confidence and self-image to allow us to achieve our potential
- Ensure everyone is important and valued
- Promote healthy lifestyles
- Encourage understanding and acceptance of individual needs
- Offer continued support for a smooth transition to the next provision


**OFSTED 2023 Overall Judgment = GOOD**
Leadership & Management = Outstanding
Behaviour & Safety of Pupils = Outstanding
Achievement of Pupils = Good
Quality of Teaching = Good

## 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 and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

## 3. Roles and responsibilities

### 3.1 The management committee

The Management Committee are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant management committee group/meeting
- Receiving (at least) basic cyber-security training to enable the Management Committee Members to check that the school meets the DfE Cyber-Security Standards
- membership of the school Online Safety Group

The management committee will support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

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

The management committee 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 committee 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 management committee member who oversees online safety is Sue Sharp. All management committee 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 5)
- 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. The designated safeguarding lead within the Online Safety Group

Details of the school's designated safeguarding lead (DSL) and deputy DSL's are set out in our child protection and safeguarding policy, as well as relevant job descriptions. Lisa Iliffe (DDSL) has the 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
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- 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
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on Schoolpod and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training online.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or management committee
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- lead the Online Safety Group
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive. (See Appendix 1 for terms of the group)

### 3.4 The ICT provider

Our technical support team MINT(Eduthing) supported by The Online Safety Lead, are responsible for:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Lisa Iliffe or Adrian Boyer, Online Safety DSL Team for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 1)
- *monitoring systems are implemented and regularly updated as agreed in school policies*
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily basis
- 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 Schoolpod 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.

### 3.5 All staff and volunteers

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

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (Appendix 8)
- they immediately report any suspected misuse or problem onto Schoolpod and DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities

- ensure learners understand and follow the Online Safety Policy and acceptable use agreements AUP (Appendices 2 to 4), have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- Knowing that the OS DSL Team (Lisa Iliffe and Adrian Boyer) are 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 contacting her immediately either by email or phone in urgent circumstances.
- Following the correct procedures by firstly requesting permission in writing from Lisa Iliffe (OS DSL) If agreed this will then be passed to MINT/Eduthing to implement any requests to bypass the filtering and monitoring systems for educational purposes
- Working with the OS DSL Team to ensure that any online safety incidents are logged on Schoolpod 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 encouraged to support the school in:

- reinforce the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)
- 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 IT systems and internet (Appendices 2 to 4)

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (Appendices 2 to 4)
- seeking their permissions concerning digital images, etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- Our school website - Online Safety Advice
- Safer Schools App - implemented school wide to provide up to date advice and information.
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

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/OSL.

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

### 3.7 Online Safety Team

The Online Safety Team has the following members:

- Designated Safeguarding Lead /Online Safety Lead
- senior leader
- online safety governor
- technical staff
- support staff

Members of the Online Safety Team will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in appendix 1

Visitors, volunteers 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 5)

See Appendix 6 and 7 for expectations around the use of Social Media

## 4. Educating pupils about online safety

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

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

**Pupils are taught a bespoke Online Safety Program.**

- Objectives are taken from **https://projectevolve.co.uk/toolkit/** and used as a starting point. Activities for each of the objectives are then planned in response to the particular needs of the current cohort due to the complex needs of our secondary pupils.

- All secondary pupils will be encouraged to use the Safer Schools app to keep up to date with current online issues.

- Primary pupils who are able, will be encouraged to use the Safer Schools app to keep up to date with current online issues.

- The safe use of social media and the internet will also be covered in other subjects where relevant.

- The school will raise pupils' awareness of the dangers that can be encountered online in all subject areas and may also invite speakers to talk to pupils about this.

- Although we cannot condone pupil use of social media accounts that they are too young to officially join, we do feel a responsibility to offer support to pupils of all ages and parents on being safe and secure.

- The safe use of social media and the internet will also be covered in other subjects where relevant.

- Due to the nature of our children, any teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with SEND.

## 5. Educating parents/carers/community members about online safety

- We provide a comprehensive collection of online safety resources on our website, which are regularly updated to reflect the latest information.

- Additionally, we offer tailored support upon request for specific online safety topics.

- Throughout the year, we host open evenings and online training sessions to further support our community.

## 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.

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, management committee members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information through the Safer Schools app, Facebook and our website 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 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”.

Pinderfields Hospital PRU 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.

Pinderfields Hospital PRU will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment and consult Lisa Iliffe (DSL) where new AI tools are being used by the PRU

## 7. Acceptable use of the internet in school

Pupils, parents/carers, staff, volunteers and management committee members are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (Appendices 5 to 8). 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, MC members 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 2 to 5

## 8. Pupils using mobile devices in school

We have carefully considered how this is managed on our premises as we are aware many pupils have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). Pupil use of mobile phones is covered in the AUP (Appendix 4)

- Pupils may bring mobile devices into school, but must hand them in on arrival and then collect them at the end of the school day.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (Appendices 2 to 4)
- 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
- Immediately reporting the loss or theft of a mobile device to DSL/OSL, Lisa Iliffe within term time school hours. Outside of these times the Headteacher, Helen Mumby, should be called regardless of the time of day or night, on 07975687890. This allows then device to be remotely wiped.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

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 8.

If staff have any concerns over the security of their device, they must seek advice from the DSL responsible for Online Safety, Lisa Iliffe.

School Google accounts/emails etc must not be accessed on personal devices.

## 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 acceptable use and behaviour policies. 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 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 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 receive refresher training at the start of the 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

MC 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. Online Safety Education Programme

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways

- A planned online safety curriculum for all sites matched against the nationally agreed framework, Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and is regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related, build on prior learning, address pupil incidents and are inclusive of Special Needs
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme is accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.

- pupils are helped to understand the need for the acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- staff act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff are vigilant in supervising the pupils and monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff are able to request the temporary removal of those sites from the filtered list for the period of study.

## 13 Filtering and Monitoring arrangements

The school filtering and monitoring provision is agreed by senior leaders, the management committee and our IT Service Provider and is regularly reviewed throughout the year and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems:

- The OS DSL Team have lead responsibility for safeguarding around online safety
- IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced

### 13.1 Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE **Filtering standards for schools and colleges**
- illegal content (e.g., child sexual abuse images) is filtered through our filtering provider Surfprotect by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective - need a written/computer method
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes - need process putting in written form as currently verbal
- filtering logs are regularly reviewed the school's IT Provider

- the school has provided differentiated user-level filtering for different groups of users.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

### 13.2 Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school uses SENSO to monitor network use across all its devices and services.
- Monitoring reports are produced:
  Non-Critical reports are addressed at the end of each day
  Critical reports cause a real time notification to be sent to both DSL members of the Online Safety Team.
  Reports are picked up, acted on and outcomes are recorded by the OS DSL, all users are aware that the network (and devices) are monitored both in school and out.
- There are effective protocols in place to report abuse/misuse.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school uses a range of appropriate strategies:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders

Online, film and gaming issues are reported using our SchoolPod MIS system. This alerts the DSL responsible for Online Safety immediately. They will then decide on what action should be taken and inform the head teacher.

For more information please see our Filtering and Monitoring Policy

## 13. Video and digital images

The school informs and educates users about possible risks and has policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with permissions held.

- Written permission from parents or carers will be obtained before photographs of pupils are used in school or published on the school website/social media.
- images will be securely stored in line with the school retention policy

## 15 Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Our public-facing website
- Our public and private social media
- Our public facing YouTube channel

The school website is managed/hosted by "Webanywhere". The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

## 16 Professional Online Safety Helpline

This is a free service to support the online safeguarding of both children and professionals The professionals online safety helpline (POSH) is a free support service for the whole of the children's workforce in the UK, the helpline plays a unique role in the online safeguarding of both children and professionals. POSH has a strong relationship with industry.
POSH has named contacts within companies such as Facebook, Instagram, WhatsApp, Twitter, Google, Roblox and so on. This gives them a unique opportunity to escalate content for removal when normal reporting routes do not work.

**The helpline is open from Monday to Friday from 10 am to 4 pm.**
**Call 0344 381 4772 or email helpline@saferinternet.org.uk.**

This policy will be reviewed every year by the DSL responsible for Online Safety. At every review, the policy will be shared with the Management Committee. The review will consider and reflect the risks pupils face online and any incidents. This is important because technology, and the risks and

harms related to it, evolve and change rapidly.

## Appendix

**The appendices are as follows:**

A1 - Online Safety Group Terms of Reference

A2 - KS1 Acceptable Use Policy

A3 - KS2 Acceptable Use Policy

A4 - KS3/4 Acceptable Use Policy

A5 - Staff/Volunteer/Management Committee Acceptable Use Policy

A6 - WMDC Social Media Policy

A7 - School Social Media Account Policy

## Appendix 1: Online Safety Group Terms of Reference

**1. Purpose**

To provide a consultative group that has wide representation from the [schools] community, with responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives.

**2. Membership**

1. The online safety group will seek to include representation from all stakeholders. The composition of the group should include.
    - SLT member/s
    - Designated SaferTeaching staff member
    - Support staff member
    - Online safety coordinator (not ICT coordinator by default)
    - Management Committee member
    - Parent/Carer
    - ICT Technical Support staff (where possible)

2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

4. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

**3. Functions**

These are to assist the DSL with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety.
- Staff training/meetings/briefings
- Management Committee meetings
- Surveys/questionnaires for learners, parents/carers and staff
- Parent/carer sessions
- Website/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- With the IT Service Provider and MC member, to carry out checks on filtering and monitoring systems
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor incidents involving online bullying

**4. Amendments**

the current needs of all committee members, by agreement of the majority.

Approved by (SLT): _____

Date: _____

Date for review: _____

**Appendix 2: KS1 Acceptable Use Policy**

**My name is _____**

1. I will only **USE** devices or apps, sites or games if I am allowed to
2. I will **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused
3. I will look out for my **FRIENDS** and tell someone if they need help
4. If I get a **FUNNY FEELING** in my tummy, I will talk to an adult
5. I **KNOW** that online, people aren't always who they say they are and

things I read are not always **TRUE**

6. I know that anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS** unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES**, even if someone tells me I must.
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** my personal information or other people's stories and photos
11. I am **KIND** and polite to everyone

**My trusted adults are:**

**_____ at school**

**_____ at home**

## Parent or Guardian Permission

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to IT systems at school.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

**Where can I find out more?**

If you or your parents/carers want to find out more, they can read the full Online Safety Policy on our website, www.pinderfieldshospitalpru.co.uk

## Parent or guardian name:

## Parent or guardian signature:

## Date:

## Appendix 3: KS2 Acceptable Use Policy

**These statements can keep me and others safe & happy at school and home**

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
5. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

6. ***I am a secure online learner*** – I keep my passwords to myself/trusted adult and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
10. ***If I make a mistake I don't try to hide it but ask for help.***
11. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
12. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
13. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
14. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
15. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
16. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
17. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
18. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
19. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
20. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
21. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
22. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
23. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
24. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
25. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
26. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure, I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~

**I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school that might mean _____**

**Outside school, my trusted adults are_____**

**Signed: _____ Date: _____**

**Parent or Guardian Permission**

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to IT systems at school.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

**Where can I find out more?**

If you or your parents/carers want to find out more, they can read the full Online Safety Policy on our website, www.pinderfieldshospitalpru.co.uk

**Parent or guardian name:**

**Parent or guardian signature:**

**Date:**

## Appendix 4: KS3/4 Acceptable Use Policy

We ask all children, young people and adults involved in the life of Pinderfields Hospital PRU to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks.

**Why do we need an AUP?**

These rules have been written to help keep everyone safe and happy when they are online or using technology. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe. But you should not behave any differently when you are out of school or using your own device or home network, either.

**"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."**

**Where can I find out more?**

If you or your parents/carers want to find out more, they can read the full Online Safety Policy on our website, www.pinderfieldshospitalpru.co.uk

**What am I agreeing to?**

1. I will treat myself and others with respect at all times; when I am online or using a device, I will treat everyone as if I were talking to them face to face.
2. I will consider my online reputation with everything that I post or share – I know anything I do can be shared and could stay online forever (even on Snapchat or if I delete it).
3. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
4. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling.
5. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
6. If I see anything that shows people hurting themselves or encourages them to do so, I will report it on the app, site or game and tell a trusted adult straight away.
7. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
8. I will only use the school's internet and devices for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or after school.
9. I understand that all internet and device use in school may be subject to filtering and monitoring.
10. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
11. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
12. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
13. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
14. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources (see fakenews.lgfl.net for support).
15. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
16. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
17. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions (many social media sites are 13+) and I should respect this. 18-rated games are not more difficult, but are inappropriate for young people.
18. When I am at school, I will only e-mail or contact people as part of learning activities.

19. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
20. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
21. I will not download copyright-protected material (text, music, video etc.).
22. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
23. Live streaming can be fun but I always check my privacy settings and know who can see what and when. If I live stream, my parents/carers know about it.
24. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.
25. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
26. I will hand in any personal mobile/smart devices on arrival at school.
27. I will only use my personal devices (mobiles, smartwatches etc) in school if I have been given permission, and I will never take secret photos, videos or recordings of teachers or students.
28. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
29. I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
30. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
31. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
32. I don't have to keep a secret or do a dare or challenge just because a friend tells me to – real friends don't put you under pressure to do things you don't want to.
33. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
34. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
35. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get in touch with Childline, The Mix, or The Samaritans.

AI is an amazing tool that can help you with learning, creating, and exploring new ideas. However, just like with any powerful tool, it's important to use AI safely and responsibly. Here's how you can do that:

1. **Think Before You Use AI:** Always ask yourself why you're using AI and how it might help you. Make sure it's for a good reason, like learning something new or solving a problem.
2. **Protect Your Privacy:** Don't share personal information with AI tools. Just like you wouldn't give out your address or phone number to a stranger, keep your details private when using AI.
3. **Check Your Sources:** AI can help find information, but it doesn't always get it right. Make sure to double-check facts from reliable sources, especially for schoolwork.
4. **Be Kind and Respectful:** If you're using AI to chat or create, remember to be respectful. Don't use AI to say or create anything hurtful or harmful to others.
5. **Ask for Help When You Need It:** If you're unsure about using an AI tool or something doesn't feel right, talk to a teacher or a trusted adult.

**I have read and understood these rules and agree with them.**

**Signed: _____ Date: _____**

## Appendix 5: Staff/Volunteer Management Committee Acceptable Use Policy

### STAFF ACCEPTABLE USE POLICY (AUP)

This acceptable use policy (AUP) is a framework for all staff and volunteers. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that PHPRU systems and users are protected from accidental or deliberate misuse that could put the security of systems and users at risk.

- that staff and volunteers are protected from potential risk in their use of technology in their everyday work.

Any concerns or clarification should be discussed with L Iliffe, the School Online Safety Lead or Shaun Booth, Head Teacher

Professional and Personal Safety:
The school's business manager manages access to the school's ICT facilities for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

- Immediately reporting the loss or theft of a mobile device to DSL/OSL, Lisa Iliffe within term time school hours. Outside of these times the Headteacher, Shaun Booth, should be called regardless of the time of day or night, on 07354318309. This allows then device to be remotely wiped.
- Teaching staff are allocated a laptop for use both in and out of school. Should other staff need to complete work at home that is related to school, they should seek permission from the Head Teacher or Online Safety Lead.
- PHPRU insurance covers the use of the ICT equipment at the staff member's home. The insurance does not cover damage/loss in transit between the school and the teacher's home. I understand that IT equipment must not be left unattended at any time outside of the home or workplace, eg in a vehicle.
- Usernames or passwords must not be disclosed to anyone else, or any other person's login used, written down or stored.
- Any supply teachers or visitors to the school must see the Business Manager to obtain details of the guest account.
- Illegal, inappropriate or harmful material or incidents must be reported immediately.

Use of Phones and Email

- 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.
- Staff should be cautious with email content to avoid potential legal claims related to discrimination, harassment, defamation, confidentiality breaches, or contract violations.
- When sending sensitive information via email, encrypt attachments as per the PHPRU Data Protection Policy.

- If staff send an email in error that contains the personal information of another person, they must inform the business manager or head teacher immediately and follow our data breach procedure.

- 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.
- Emails should be treated as potentially retrievable and disclosed in legal proceedings or data protection requests similar to paper documents under the Data Protection Act 2018.

**Personal Use**

Staff are permitted to occasionally use school IT facilities for personal use, subject to certain conditions set out below.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined above
- Takes place when no pupils are present
- Does not interfere with their work, or prevent other staff or pupils from using the facilities for work or educational purposes

**Personal Device Use**

- Personal mobile devices must not be used in areas of school with pupil access, unless **specific** authorisation has been given by the Head Teacher or Online Safety Lead.
- During lessons, mobile phones must be turned off/put on silent mode and stored away in a cupboard or drawer etc, unless **specific** authorisation has been given by the Head Teacher or Online Safety Lead.
- Adults must only access their personal devices on breaks, lunch times and after school in safe, suitable places where the pupils are not present.
- Personal equipment must not be connected to PHPRU equipment or wifi without prior approval from Online Safety Lead or MINT technician.
- It is forbidden to take photographs/videos of pupils on personal mobile devices. In an emergency, authorisation may be given by the Head Teacher or Online Safety Lead.

I will be professional in my communications and actions when using *PHPRU* systems:

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the following:
    - All images and videos of pupils should be taken only on designated devices
    - Permission from pupils/parents/staff must be gained before using any images or videos.
    - Permissions can be found for pupils on SchoolPod and on the New Staffroom GDrive for staff
    - All images/videos taken on will be saved to Google Photos accounts for each site.

- I will only use social networking sites in school in accordance with the following:
    - You must not add a pupil/parent to your 'friends list', nor invite them to be friends with you.
    - Guidelines set out in the staff code of conduct, should be followed with regard to contact/relationships with past students.
    - Personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
    - Employees must not post any school/council information or logos online without the express permission of the head teacher or other authorised personnel.
    - You must ensure that any private social networking sites/blogs that you create or contribute to are not to be confused with your professional role in any way.
    - When posting online, avoid content that could be mistaken as representing PHPRU, harm the school's reputation, or disclose personal information that could lead to embarrassment, harassment, or defamation.

- I will only communicate with students/pupils and parents/carers using official school systems. Communications will be professional in tone and manner and will be recorded on Schoolpod. Staff (including management committee and non-teaching staff) must not use personal email accounts/mobile phones/social media accounts for any school/work related activity – no exceptions!
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- This is in conjunction with Wakefield Councils Social Media Policy for School Employees (attached)

PHPRU and the local authority have the responsibility to provide safe and secure access to technologies:

- I will avoid opening any email attachments or hyperlinks unless I trust the source to prevent potential risks such as viruses.
- If I receive any unsuitable communications I will report them immediately.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that pupils must be supervised by staff at **all times** when using the internet.
- When searching the internet with pupils, I will encourage pupils to use 'child safe' search engines. Any opportunity to have discussion around Online Safety topics should be used.

- The school uses the SaferSchools app for online safety, accessible on personal devices or PHPRU devices. The app ensures GDPR compliance, allows targeted information delivery within the organisation.

**Storage of Documents and Data:**

- Memory sticks and other external storage must not be used with school equipment. Should the need for an encrypted stick arise, you should obtain one from the Business Manager
- Documents and data of any nature should be stored either using Google Drive or the PHPRU server.
- Server – storage can be accessed using school computers and laptops on all sites. The server has a high level of security and staff laptops have been encrypted to protect confidential data.

- Google Drive – Storage is available to all staff through their Google account. This is the preferred area for storage as it is accessible anywhere with an internet connection using equipment supplied by Pinderfields Hospital PRU.

Reporting Procedures for Incidents or Security breaches:

- OS incidents should be regarded as safeguarding incidents reported as soon after the incident as possible, including incidents outside of school.

- If a Safeguarding Slip has been completed and contains elements of OS, an IT Incident Slip should also be completed with a sentence referring it to the Safeguarding Slip.

**School Social Media Accounts:**

Currently, we have three social media accounts.

- **X** - an account set up to provide parents with information and share images of the school day, enabling us to communicate more effectively.
- **Facebook** - our public page shares general information, while closed groups are site-specific for confidential communication with parents. Staff can join using approved professional accounts.
- **Youtube** - a school channel to publish video content. Each site has a playlist allowing them to cater to their audience

Please see our separate Social Media Policy for further details of these platforms.

**Artificial Intelligence (AI)**

It is important to keep our community informed about the different types of Artificial Intelligence (AI) and their potential impact. AI is increasingly integrated into various aspects of our digital lives, and understanding its different types can help us navigate technology safely and responsibly for our professional use and the safeguarding of our pupils.

AI technology advancements bring new applications and challenges for schools. PHPRU is responding with guidance and updates. Contact MINT or the Online Safety Lead before using AI in school with pupils.

**Filtering & Monitoring**

The implementation of Filtering and Monitoring Standards is designed to create a safe and secure learning environment for all members of our mixed-age school community. By adhering to these standards, we aim to promote responsible and ethical use of technology and protect our students from exposure to harmful content. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed.

Practicalities of Filtering & Monitoring for Staff

- On a Windows device with SENSO installed all usage is monitored. This is system wide and includes all web traffic and usage of the device both on and off site.
- SENSO has the ability to take screenshots of the user's device should breaches occur.
- On an iPad, due to the restrictions that Apple have in place, only web traffic is monitored by SENSO.
- All devices in school are subject to filtering at network level. This is all network traffic on the device and includes personal devices connected to the school's network, which should only happen with the Online Safety Leads approval

**Review and Evaluation**
This policy will be reviewed annually or in response to a relevant incident.

Please complete and sign the sections below. This page should then be returned to Lisa Iliffe, Online Safety Lead.

Alternatively, it can be completed on line using this link https://forms.gle/Ftr6JFHT1hAuGPve7
I have read, understood and agree to comply with the 25/26 AUP:

Signed: _____

Print Name: _____

Position in School: _____

Site:_____

Date: _____

**Image and Video Permissions**
PLEASE DELETE AS APPROPRIATE

I give / do not give permission for my image to be used on the school website staff list

I give / do not give permission for my image/video to be used on the school website.

I give / do not give permission for my image/video to be used on the school public Facebook page

I give / do not give permission for my image/video to be used on the private parent Facebook groups

I give / do not give permission for my image/video to be used on the school Youtube channel

I give / do not give permission for my image/video to be used on the school Twitter account

I give / do not give permission for the continued use of my image/video for a reasonable time. (eg in the background of an image etc?

I will / will not be installing The Safer Schools app on my personal device.

Signed: _____

Print Name: _____

## APPENDIX 6: **WMDC Social Media Policy**

## APPENDIX 7: **School Social Media Account Policy**

### SCHOOL SOCIAL MEDIA ACCOUNTS

- **X (Formally Twitter)** - set up to provide parents with information and share images of the school day, enabling us to communicate more effectively.
- **Facebook** - used to post general information that is appropriate for public viewing.
- **Facebook Groups** – used by Woodlands, Thornes, Forest Wood, EYAC and the Wrenthorpe Centre to communicate with parents, sharing images and information. These groups are private and only available to current parents/carers of pupils within the setting.
- **YouTube** – used to publish media content. This account has the ability to post both privately and publicly.

### ACCESS TO SCHOOL SOCIAL MEDIA ACCOUNTS

- The Online Safety Lead, Headteacher, Assistant Headteachers and Teachers in Charge and Parent Support Workers have admin access to school social networking private accounts on school owned devices.
- The Online Safety Lead, Headteacher, Assistant Headteachers have admin access to school social networking public accounts on school owned devices.

- Other staff and students have viewing only access.

## CONTENT OF SCHOOL SOCIAL MEDIA ACCOUNTS

- Content on all platforms will be monitored regularly by the Online Safety Lead, Headteacher and Assistant Headteacher.
- Posts on our social media accounts will not include names of staff, children or their families, unless specific permissions are in place.
- Posts within the private Facebook groups may contain names due to the closed nature of the group and how members are approved.
- All pictures must be checked for permissions before publishing, even if the child/staff member is simply in the background of the image.
- Posts must be professionally written with the reputation of the school in mind at all times. Posts or messages will be removed if they are deemed to contradict any of the above. Members will then be removed from groups and staff members will face formal action.

## ACCESS TO CONTENT ON SCHOOL ACCOUNTS

- X - all content on the school account is public. This means it can be viewed by anyone.
- Facebook - all content on the school page is public. This means it can be viewed by anyone.
- Facebook Groups - Only members of the groups can view the content. People requesting to join the group must be verified as a parent/guardian of a child currently on role. Any specific parental restrictions for that child should be checked by the TIC prior to admission being granted. Once members of the closed group, parents are able, and should be encouraged to, share images and posts in the group. Permissions must be in place for the PRU to post images within the groups. Use of images that have been uploaded by parents outside of the group require extra permissions in place. Each year a new group will be created for each site, this stops past/present parents seeing past/present images. Once a child leaves the school, it is the TIC's responsibility to remove their parents from the group immediately.

## ACCEPTABLE USE POLICY

- Staff - All of the content in this policy is summarised and included in the staff, volunteer and Management Committee AUP. This works in conjunction with Wakefield Council's Social Media Policy for School Employee's which can be found on the Traded Services Portal.

## CHILD IMAGE CONSENT

- Consent is gained from parents for all pupils in the Pupil Induction Pack. This consent must be in place and checked before any content is published. Permissions can be checked on the individual pupil profiles within Schoolpod.

**COMPLAINTS PROCEDURE**

- If a Parent or Carer has any concerns or complaints with regard to social media, an appointment can be made by them to speak to the Headteacher, Assistant Headteacher or Online Safety Lead, who will investigate the complaint and if necessary advice on formal procedures for complaint.

**BREACHES OF POLICY**

- Any breaches of policy not already detailed above will be dealt with by the Headteacher accordingly.

**REVIEWING THIS POLICY**

This policy will be reviewed annually by the Online Safety Lead. It will then be shared with the Head and sent to the Management Committee for ratification. Once it has been ratified, a copy will be given to all staff and made publicly available