HEREFORDSHIRE PUPIL REFERRAL SERVICE

HPRS

E-SAFETY POLICY

Version: FEBRUARY 2023

Status	Statutory
Responsible Management Committee (MC)	Curriculum
Date last approved by MC	
Responsible Person	Headteacher
To Review Date	FEBRUARY 2025
Last Amended Date	FEBRUARY 2023

CONTENTS

SECTION A: POLICY & LEADERSHIP

Background & Rationale

The potential that technology has to impact on the lives of all of us increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content;
- Allowing or seeking unauthorised access to personal information;
- Allowing or seeking unauthorised access to private data, including financial data;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are a member of the Herefordshire Pupil Referral Service (HPRS). We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our e-safeguarding policy has been derived from a model provided by the South West Grid for Learning.

Responsibilities

The HPRS leadership team (which includes the e-safety coordinator) regularly discusses issues relating to e-safety. Issues may also be raised at weekly meetings attended by staff. Issues that arise are referred to other bodies as appropriate and when necessary to bodies outside the Centre such as Herefordshire's Safeguarding Children Board (HSCB).

The E-Safety Co-ordinator

Our E-Safety Co-ordinator is the person responsible for the day to day issues relating to e-safety. This is currently the Headteacher. The e-safety co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident;
- provides training and advice for staff;
- liaises with the Local Authority;
- liaises with ICT technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- reviews regularly the output from monitoring software and initiates action where necessary;
- reports regularly to the Senior Leadership Team;
- receives appropriate training and support to fulfil their role effectively.

The Head of Centre

- The Head of Centre is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day-to-day responsibility for e-safety is delegated to the E-Safety Co-ordinator.
- The Head of Centre and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff (see flow chart on dealing with e-safety incidents (included below) and other relevant Local Authority HR / disciplinary procedures).

Classroom-based Staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**;
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the service's Acceptable Use Agreement for staff;
- they report any suspected misuse or problem to the E-Safety Co-ordinator;
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems;
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme.

ICT Technical Support Staff *(including outsourced providers)*

The ICT Technical Support Staff are responsible for ensuring that:

- the service's ICT infrastructure and data are secure and not open to misuse or malicious attack;
- the service meets the e-safety technical requirements outlined in Section B of this policy (and any relevant Local Authority E-Safety Policy and guidance);
- users may only access the service's networks through a properly enforced password protection policy as outlined in the E-Security policy;
- shortcomings in the infrastructure are reported to the Head of Centre so that appropriate action may be taken.

Policy Scope

This policy applies to **all members of the HPRS community** (including teaching staff, wider workforce, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, **both in and out of school**.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place away from our sites, but are linked to membership of the service.

The service will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place away from our sites.

Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils;
- Staff (and volunteers);
- Parents / carers;
- Community users of the Centre's ICT system.

Notes on Acceptable Use Agreements:

- Acceptable Use Agreements are introduced at admission meetings and signed by all pupils as they join the Centre;
- All employees of the service and volunteers sign when they take up their role and in the future if significant changes are made to the policy;
- Parents sign once when their child joins HPRS. The parents' policy also includes permission for use of their child's image (still or moving) by the service, permission for their child to use the service's ICT resources (including the internet) and permission to publish their work;
- Community users sign when they first request access to the service's ICT system;
- Induction policies for all members of the school community include this guidance.

Illegal or Inappropriate Activities & Related Sanctions

HPRS believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using the service's equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images** *(illegal - The Protection of Children Act 1978)*
- **grooming, incitement, arrangement or facilitation of sexual acts against children** *(illegal – Sexual Offences Act 2003)*
- **possession of extreme pornographic images** *(illegal – Criminal Justice and Immigration Act 2008)*
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)** *(illegal – Public Order Act 1986)*
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the service or brings the service into disrepute

Additionally, the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the service:

- Using HPRS systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the service (or its support service providers)
- Uploading, downloading or transmitting commercial software or copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line gambling
- On-line shopping / commerce (unless carried out for the related operations of the service)
- Use of social networking sites (other than on sites otherwise explicitly permitted by the service)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

It is more likely that the service will need to deal with incidents that involve *inappropriate* rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the HPRS community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as indicated on the following pages.

Student sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They will be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Refer to:					Inform:	Action:		
	Class teacher	E-safety coordinator	Refer to Head of Centre and/or Head Teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons without permission	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔							✔	
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access the service's network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the service's network, using another pupil's account	✔				✔		✔		
Attempting to access the service's network, using the account of a member of staff	✔		✔		✔	✔	✔	✔	
Corrupting or destroying the data of other users	✔		✔		✔	✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔		✔
Actions which could bring the service into disrepute or breach the integrity of the ethos of HPRS	✔		✔					✔	
Using proxy sites or other means to subvert the service's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔			
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔		✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔		✔		✔		

Staff sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They will be applied according to the context of any incident and in the light of consequences resulting from the offence.

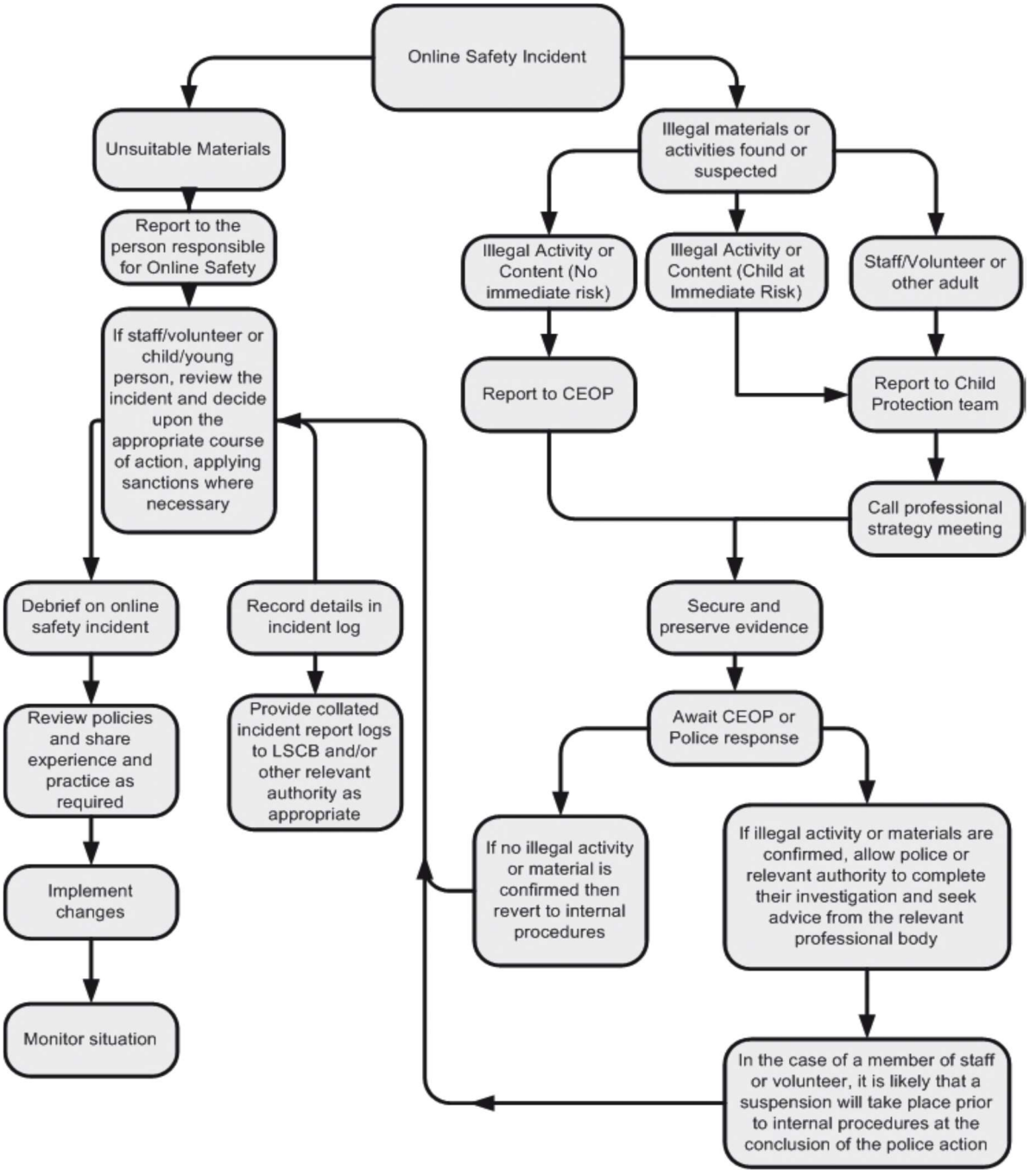
	Refer to:					Action:		
	Line Manager	Head of Centre and/or Head Teacher	Local Authority / HR	Refer to Police	E-safety coordinator / Technical Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
Allowing others to access the service's network by sharing username and passwords or attempting to access the network using another person's account	✔	✔			✔	✔	✔	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	✔	✔
Using personal email / social networks / instant or text messaging to carrying out inappropriate digital communications with pupils	✔	✔			✔			
Actions which could compromise the staff member's professional standing	✔	✔						
Actions which could bring the service into disrepute or breach the integrity of the ethos of HPRS	✔					✔		
Using proxy sites or other means to subvert the service's filtering system	✔				✔	✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations	✔					✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

Reporting of E-Safety Breaches

It is hoped that all members of the HPRS community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. The diagram below shows the responses that will be made to any apparent or actual incidents of misuse.

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section earlier in this policy.

Reporting Process Diagram for E-Safety Breaches:



Use of Hand Held Technology

We recognise that the area of mobile technology is rapidly advancing and it is HPRS policy to review its stance on such technology on a regular basis. Currently our policy is this:

- **Members of staff** are permitted to bring their personal mobile devices into the centres. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking our advice is that:
  - ✓ Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances.
  - ✓ Members of staff are free to use these devices outside teaching time.
  - ✓ Under no circumstances should images or video of students be captured or stored on the personal mobile devices of members of staff.
  - ✓ A school mobile phone is available for professional use by staff (for example when engaging in off-site activities).
- **Pupils** are not currently permitted to bring their personal hand held devices into the centre – devices are collected from pupils at the start of the school day and returned when they leave.
- **Pupils at KS4** are free to use these devices at lunch time, but they must be handed-in again before the afternoon session. See the KS4 Behaviour Policy for how to handle breaches of this rule.
- A number of such devices may be available in school (e.g. PDA, I-pod Touch) and are used by pupils as considered appropriate by members of staff.

Personal hand held technology	Staff / Adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought into the Centre	✔					✔ KS4		✔ KS3
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time		✔				✔ KS4		✔ KS3
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles	✔						✔	

Use of Communication Technologies

Email

Access to email is provided for all users at HPRS, managed by our support service provider. These official email services may be regarded as safe and secure and are monitored.

The following notes apply to the use of email services at HPRS:

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy).
- Staff are permitted to access personal email accounts on school systems within the boundaries of the service's acceptable use policy (if they are not blocked by filtering).
- Users must immediately report to their class teacher / e-safety coordinator - in accordance with the service policy - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

Use of Email	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts on service's network		✔						✔
Use of HPRS email for personal emails		✔						✔

Social Networking (including chat, instant messaging, blogging etc)

Use of Social Networking Tools	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non educational chat rooms etc				✔				✔
Use of non educational instant messaging		✔						✔
Use of non educational social networking sites		✔					✔	
Use of non educational blogs		✔						✔

Use of Digital Video and Images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images (see section C of this policy). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Members of staff are allowed to take digital still and video images to support educational aims, but must follow the service's policies concerning the sharing, distribution and publication of those images. Those images should only be captured using HPRS equipment; **the personal equipment of staff should not be used for such purposes.**

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission

Sexting

A young person taking an indecent image of themselves and sending to their friends or boyfriend / girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'Sexting'. Young people need to be aware that they could potentially be distributing illegal child images. Staff working at HPRS will ensure that our young people are aware of the risks associated with the use of the internet, including sexting, and guidance is issued to staff on how to respond appropriately to a 'Sexting' incident. We know this can cause enormous distress to children and young people and may place them at risk of sexual grooming and other risks associated with the internet.

We use guidance produced by the UK Council for Internet Safety (*"Sharing nudes and semi-nudes: advice for education settings working with children and young people"*) as the basis for our procedures of how to respond to incidents of this type. The document can be found online here:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

Issues around sexting are taught to all our pupils through the ICT curriculum and dedicated e-safety lessons.

Use of Web-based Publication Tools

Website

The HPRS uses public facing websites only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children.

All users are required to consider good practice when publishing content, according to the following guidelines:

- Personal information will not be posted on the HPRS website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupils' first names will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - ✓ Where possible, photographs will not allow individuals to be recognised
    - ✓ Written permission from parents or carers will be obtained before photographs of pupils are published on the website (see Appendix 1)
- Pupils' work can only be published with the permission of the pupil and parents or carers. (see Appendix 1).

Professional Standards for Staff Communication

In all aspects of their work in HPRS, teachers abide by the **Teachers' Standards** as described by the DfE: http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.

Teachers translate these standards appropriately for all matters relating to e-safety.

In addition, all staff are expected to conform to **Herefordshire Council's Code of Conduct**, which is adopted in full by HPRS and includes conduct expectations around communication and use of technology.

Any digital communication between staff and pupils or parents/carers (email, chat, learning platform etc) must be professional in tone and content.

- These communications may only take place on official (monitored) service systems.
- Personal email addresses, text messaging or public chat / social networking technology should not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

SECTION B: INFRASTRUCTURE

Password Security

This is dealt with in detail in our school's *E-Security Policy*. Please refer to that document for more information.

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy).

Filtering

Introduction

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. It is therefore important that the service has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in HPRS.

As a school using broadband services through Herefordshire Council service providers, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

It is recognised that HPRS can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **E-safety Co-ordinator** (with ultimate responsibility resting with the **Head Teacher** and **Management Committee**). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Herefordshire school filtering service will:

- be logged in change-control logs
- be reported to a second responsible person *(the Head Teacher)*

All users have a responsibility to report immediately to class teachers / E-safety Co-ordinator any infringements of the service's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education, Training & Awareness

Pupils are made aware of the importance of filtering systems through the e-safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing updates in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the service's filtering policy through the Acceptable Use Agreement (Appendix 1)

Changes to the Filtering System

Where a member of staff requires access to a website that is blocked for use at HPRS, the process to unblock is as follows:

- A member of teaching staff requiring access to a website for use at school that is blocked should:
- Contact their own school e-safety coordinator who should check the website content and agree if it is appropriate for use at the school or not.
- If agreement is reached, the e-safety coordinator should log the request with the IT Support Helpdesk on **03306 062 650** or email **support@dandd.org.uk**
- Helpdesk staff will endeavour to unblock the site within 24 hours. (This process can still take a number of hours so teaching staff are still asked to check websites in advance of teaching sessions).

The e-safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests (see separate guidance document) but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for students.

Monitoring, Auditing & Reporting

No filtering system can guarantee 100% protection against access to unsuitable sites. The service will therefore monitor the activities of users on the service's network and on equipment.

Monitoring takes place as follows:

- Identified member(s) of staff reviews the Policy Central console captures weekly
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.

Filter change-control logs and incident logs are made available to:

- the Head of Centre and Head Teacher
- the Management Committee
- the Herefordshire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

Technical Security

This is dealt with in detail in the service's E-Security Policy. Please see that document for more information.

Personal Data Security (and Transfer)

This is dealt with in detail in the service's E-Security Policy. Please see that document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy).

SECTION C: EDUCATION

E-safety Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the service's e-safety provision. Children and young people need the help and support of HPRS to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- An e-safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both within HPRS and outside.
- Key e-safety messages will be reinforced through further input via pastoral activities, as well as informal conversations when the opportunity arises.
- We use the resources on the Child Exploitation & Online Protection Centre's (CEOP) 'Think U Know' website as a basis for our e-safety education *http://www.thinkuknow.co.uk/teachers/resources/*
- Pupils will be helped to understand the need for the pupils' Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within HPRS and outside.
- In lessons where internet use is pre-planned, it is best practice that pupils should be 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

Information Literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
  - ✓ Checking the likely validity of the URL (web address)
  - ✓ Cross checking references (Can they find the same information on other sites?)
  - ✓ Checking the pedigree of the compilers / owners of the website
  - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

The Contribution of Pupils to E-learning Strategy

It is our general policy to encourage pupils to have a say in shaping the way HPRS operates and this is very much the case with our e-learning strategy. Our pupils often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Staff Training

It is essential that all staff – including non-teaching staff - receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Dedicated e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Centre's e-safety policy and acceptable use policies which are signed as part of their induction.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- The E-safety Co-ordinator will be CEOP trained.

Parent & Carer Awareness Raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" *(Byron Report)*.

The Centre will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and our website
- Parent/carer meetings and open afternoons

Wider School Community Understanding

HPRS will strive to offer, or provide access to, family learning resources in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and others. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access the service's ICT systems / website / learning platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to the HPRS systems.

SECTION D:
REMOTE LEARNING – SAFEGUARDING PUPILS & STAFF

HPRS has developed a dedicated Remote Learning Policy, which is available to view separately. This section of our e-safety policy deals with the safeguarding principles around remote learning, which are also included in the Remote Learning Policy.

Communication Channels

In keeping with long-standing best practice, staff shouldn't communicate with parents or pupils outside of official school channels (e.g., they shouldn't talk to parents using personal Facebook accounts, or contact pupils using personal email addresses or phone numbers). All staff and pupils at HPRS are issued with school-based email accounts, accessible in and out of school. Communications should be conducted around normal school hours.

At HPRS we use the following platforms and communication channels:

- Email (Office 365)
- T2P (Text 2 Parents) – messaging service that can be used to contact parents/carers and pupils directly
- Phone (staff using personal devices to contact parents should do so using withheld numbers [141])
- Microsoft Teams (communication platform – messaging, meetings, classes, assignments)
- Tute (live lesson delivery platform)

Principles for the delivery of 'live' lessons / online face-to-face sessions

- Staff should:
    - Sit against a neutral background
    - Avoid recording in their bedroom where possible (if that's not possible, use a neutral background)
    - Dress like they would for school – no pyjamas!
    - Double check that any other tabs they have open in their browser would be appropriate for a child to see, if they're sharing their screen
    - Use professional language
    - Make a recording of the session and keep a log of any face-to-face sessions/video calls that are made.

For Parents/Carers & Pupils

Acceptable Use – Rules for Remote Learning

Pupils must:

- not reveal their password to anyone – their account is their responsibility.
- **ensure that all of communication with other pupils and teachers using technology is responsible and sensible – including the language that is used.**
- must not browse, download, upload or forward material that could be considered offensive or illegal. If a pupil accidentally comes across any such material, they should report it directly to a teacher or parent / carer.
- must not record or take photos of classmates or teachers during video conferencing sessions, nor share lessons publicly.
- understand that if using Microsoft Teams and other applications provided by the school that the lessons and their content are recorded and individual use can be monitored and logged.

These rules are designed to help keep all of our pupils safe online. If they are not followed, school sanctions will be applied and parents / guardians contacted. It could be that their online account is blocked.

Video Conferencing Guidelines

Teachers may incorporate video conferencing through Microsoft Teams or TUTE; remember that this is an extension of the classroom and pupils should conduct themselves as they would in a classroom. Please support this by helping to make sure pupils:

- Join Teams lessons from an environment that is quiet, safe and free from distractions ideally in a common space and within earshot of parents (and not a bedroom). A kitchen table, living room or family space is recommended.
- Are dressed appropriately for learning in home clothes (e.g. no pyjamas, no vest tops, hats or hoods).
- Remain attentive during sessions and free from distractions. For example, they should not be using personal social media in lesson time.

APPENDIX 1:

ACCEPTABLE USE POLICY AGREEMENTS

1. **Student**
2. **Parent/Carer (plus permission forms)**
3. **Staff/Volunteer**
4. **Community User**

SEE SEPARATE DOCUMENTS THAT FOLLOW