PensMeadowSchool

Living, Growing, Learning

Online Safety Policy

SEPTEMBER 2026

NEXT REVIEW DATE: SEPTEMBER 2027

Staff Responsible: Mr M. Pawlowicz

Disclaimer

Pens Meadow School makes every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by Pens Meadow School. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the school's copyright is acknowledged and we are informed of its use.

In particular this policy should be read in conjunction with the Behaviour Policy, Safeguarding policy, Staff Acceptable Use Policy (AUP/AUA) and Confidential Reporting Policy.

1. Rationale

Pens Meadow School recognises that technology is integral to communication, learning, independence, inclusion and preparation for adulthood. It can be particularly enabling for pupils who use augmentative and alternative communication, switches, eye-gaze, accessible devices, symbols, photographs, video modelling and other assistive technologies. The school will promote those benefits while taking proportionate action to prevent, identify and respond to harm.

Online safety is safeguarding. The same professional curiosity, child-centred practice, recording and escalation apply to concerns that arise online and offline.

The school will:

- protect pupils from illegal, inappropriate and harmful content, contact, conduct and commerce risks;
- teach online safety in a developmentally appropriate, accessible and frequently revisited way;
- avoid restricting beneficial learning or communication more than is necessary;
- make reasonable adjustments so pupils can report concerns using their preferred communication method;
- work with parents, carers, social care, police, health professionals, the local authority and technology providers where appropriate;
- keep technical controls, staff supervision and curriculum provision under regular review.

2. Scope

This policy applies to pupils, staff, governors, volunteers, agency workers, contractors, visitors, parents/carers and community users. It applies to school systems, school-managed devices and services, personal devices used on site or for school business, remote learning, school trips, transport and off-site activity where conduct affects a pupil, the school community or safeguarding.

The four areas of online risk

Area	Examples relevant to Pens Meadow
Content	Pornography; racism; misogyny; antisemitism; extremism; self-harm or suicide material; misinformation and disinformation; harmful challenges; violent content; AI-generated or manipulated content.
Contact	Grooming; exploitation; impersonation; coercion; sextortion; harmful peer contact; adults posing as children; pressure through gaming, messaging, live-streaming or social media.
Conduct	Cyberbullying; harmful sexual behaviour; creating or forwarding intimate images; oversharing; unsafe live-streaming; abusive posts; filming others without consent; use of AI to create harmful or humiliating material.
Commerce	Scams; phishing; in-app purchases; gambling-like features; financial exploitation; inappropriate advertising; identity theft; fraudulent offers.

"Online" includes internet-connected and offline digital activity, including proximity sharing, Bluetooth, AirDrop-style services, messaging, gaming, cameras, recording, wearable technology, smart devices and artificial intelligence. "Pupil" includes children and young people attending the school; safeguarding duties apply to those under 18, while concerns involving pupils aged 18 or over are managed under relevant adult safeguarding arrangements as well as school procedures.

3. Legal Framework

This policy has regard to applicable law and the most recent national guidance, including:

- Keeping Children Safe in Education 2026;
- Working Together to Safeguard Children 2023, as amended;
- DfE digital and technology standards for schools and colleges, including filtering and monitoring, cyber security, digital leadership and governance, and digital accessibility (updated August 2026);
- DfE Teaching online safety in schools;
- DfE Generative artificial intelligence in education and Generative AI: product safety standards;
- UKCIS Sharing nudes and semi-nudes: advice for education settings (updated 2024);
- DfE Searching, screening and confiscation at school;
- Prevent duty guidance;
- Education for a Connected World;
- Data Protection Act 2018 and UK GDPR;
- Computer Misuse Act 1990;
- Protection of Children Act 1978;
- Sexual Offences Act 2003;
- Voyeurism (Offences) Act 2019;
- Online Safety Act 2023;
- Equality Act 2010;
- Human Rights Act 1998;
- Education and Inspections Act 2006.

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy

4. Pens Meadow context and pupil vulnerability

Pens Meadow is a specialist school. Pupils may have severe learning difficulties, profound and multiple learning difficulties, autism, sensory or physical impairments and communication needs. Chronological age must not be treated as a reliable indicator of online understanding. Risk assessment and teaching will consider developmental level, communication, capacity, dependency on adults, sensory regulation, social understanding and any history of exploitation or trauma.

Staff will recognise that pupils with SEND may:

- be more trusting, literal or socially isolated;
- find it difficult to recognise deception, coercion, sexualised behaviour, advertising or persuasive design;
- use repetitive or highly focused online activity and find changes or restrictions distressing;
- depend on adults to access, configure or communicate through technology;
- be less able to explain what happened, identify a perpetrator or preserve evidence;
- communicate distress through behaviour, sleep changes, withdrawal, self-injury or dysregulation rather than verbal disclosure;
- have images, health information or care needs shared by adults without sufficient regard to dignity and privacy.

A disclosure may be made through speech, signing, symbols, eye-gaze, behaviour, a communication device, drawing, a photograph or a trusted adult. Staff must record the pupil's own communication accurately and avoid leading questions.

5. Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety policy and for reviewing the effectiveness of the policy. The governing body will review the Online Safety Policy at the start of each academic year to ensure that all new staff and pupils are aware of its content and have signed the appropriate Acceptable Use Agreements (Appendix 3). Governors will receive regular information about online safety incidents and monitoring reports.

Two member of the Governing Body have taken on the role of Online Safety Governors.

These governors at Pens Meadow School are Paul Leyshon and Paul Hill

The role of the Online Safety Governor will include:

- Regular meetings with Online Safety Co-ordinator
- Regular updates on the monitoring of Online safety/Smoothwall incident logs
- Regular updates on the monitoring of the filtering of web sites/change control logs
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Reporting to relevant Governor meetings

Head teacher and Senior Leaders:

The Head teacher is responsible for ensuring the safety (including Online safety) of members of the school community. The school's SIRO is responsible for reporting security incidents as outlined in the schools Information Security Policy. The day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.

- The Head teacher/SLT are responsible for ensuring that the Online safety coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils are taught how to use ICT tools such as the internet, email and social networking sites and AI tools, safely and appropriately
- The Head teacher/SLT will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

  (Guidance relating to the reporting procedure for* Online safety *incidents- see appendix 1.
- The SLT will receive regular monitoring reports from the Online Safety Co-ordinator.

  The Head teacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that parents/carers understand that the school may investigate any reported misuse of systems, by pupils, out of school hours, as part of 'safeguarding' procedures.

Online Safety Coordinator:

The school has a named person with the day to day responsibilities for Online Safety.

The Online Safety Co-ordinator at Pens Meadow School is Michal Pawlowicz, Deputy Head Teacher.

Responsibilities include:

- Taking day to day responsibility for Online safety issues and having a leading role in establishing and reviewing the school's Online safety documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority and relevant organisations
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Liaising with school contact from the managed service provider- RM
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Meeting regularly with the online Safety Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings/Governor committee meetings
- Reporting regularly to the Senior Leadership Team
- Manage the staff members with IT responsibilities

Managed service provider (applicable to RMUnify3 School):

The managed service provider is responsible for helping the school to ensure that it meets the Online Safety technical requirements outlined by RMUnify, which is aligned to national guidance. The managed service provides a number of tools to schools including Smoothwall, RMSafetyNet filtering and MDMs (Mobile Device Management systems), which are designed to help schools keep users safe *(See appendix* 2).

Schools are able to configure many of these locally or can choose to keep standard settings.

A designated adult can access activity logs for network users and apply 'rules' to specific group of users. Schools should nominate a suitable member of staff to manage this responsibility and keep logs of any changes made to filtering and monitoring rules.

CC4 Anywhere and similar products, are applications that enables a user to remotely access documents and applications stored on the school server/servers. The school has responsibility for ensuring files and applications accessed via this system comply with information and data security practices.

The RMUnify Client team work with school representatives to develop and update a range of Acceptable Use Agreements/guidance *(see Appendix 3)* and include relevant Local Authority Online Safety policies and guidance.

https://dudleysafeguarding.org.uk/children/parents-and-carers/online-safety-and-use-of-images/

Members of the RMUnify team will support school to improve their Online Safety strategy.

The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the RMUnify team.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online safety/E-Safety matters and of the current school Online safety policy and practices, including AI tools
- They have read and understood the most recent guidance specified in KCSIE (Keeping Children Safe in Education – September 2026)
- They do not bring the school to disrepute whilst using social media
- They access Microsoft TEAMS software regarding confidentiality rules, especially when accessing sensitive information
- They encourage pupils to develop good habits when using ICT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Agreements (AUA's)
- They report any suspected misuse or problem to the Online Safety Co-Ordinator for investigation / action / sanction
- Digital communications with pupils (email and school's official Social Media pages) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum
- Pupils understand and follow the school online safety and acceptable use agreements
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices, including their personally owned devices and that they monitor their use and implement current school policies with regard to the use of these devices in the school or during extended school activities. A guardianship/loan form is in use for school owned equipment used by staff - See appendix 4
- In lessons, where internet use is pre-planned, 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. They include the teaching of Online safety in their lessons (See appendix 1)
- Pupils understand, where possible, that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with the AUA
- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated Safeguarding Lead:

The named person Michal Pawlowicz is trained in Online Safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Publishing of specific information relating to school based activities involving pupils, via official school systems such as the school web site, Facebook, Instagram
- Sharing of school owned devices or personal devices that may be used both within and outside of the school
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying, Sexting and Sextortion, Revenge porn, Radicalisation, CSE

DSL is also responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and governing board to update this policy on an annual basis.

Pupils:

Pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure, monitored and safe system provided through Smoothwall. Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement/AUA *(see appendix 3*), which they, or their parents/carers will be expected to sign before being given access to school systems through the schools home to school agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites, video streaming facilities, digital image sharing sites and cyber-bullying. This includes the implications of use outside of school.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to the use of an externally available web-based system, provided by the school
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local Online/E-Safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Agreement through the schools Home to school agreement
- Accessing the school website in accordance with the relevant school Acceptable Use /AUA.
- Promoting good online safety practice by following guidelines on the appropriate use of digital and video images taken at school events and their children's devices in school.

Community Users/ 'Guest Access':

Community Users who access school ICT systems and associated software and records as part of the Extended School provision will be expected to sign a Community User AUA before being provided with access. See appendix 3.

6. Education and Training

Pupils

Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. All staff have a responsibility to promote good Online/E-safety practices.

Online safety education is provided in the following ways:

- A planned Online Safety programme is provided as part of the schools PHSCE curriculum and is regularly revisited – this includes the use of ICT and new technologies in and outside the school.
- Key Online safety messages are reinforced as part of assemblies and pastoral activities
- At Pensnett Site Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
- Pupils are aware, where cognitively able, of the Pupil AUA's and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school
- Pupils are aware, where cognitively able, that their network activity is monitored and where pupils are allowed to freely search the internet their internet activity is being scrutinised
- Pupils may need to research topics that would normally be blocked and filtered. Any request to unfiltered blocked sites for a period of time, must be auditable
- Rules for use of ICT systems and internet are posted in all rooms
- Pupils, where cognitively able, are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Parents / Carers

The school provides information and awareness to parents and carers through:

- Letters, newsletters, school web site, official school/academy social networking sites
- Parents evenings, Induction meetings
- Online/E-Safety sessions for parents/carers
- Family learning opportunities

Extended Schools/Wider Community

The school offers family learning courses in ICT, computing, digital literacy and Online Safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around Online Safety are targeted towards grandparents and other relatives as well as parents/carers.

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.

Staff/Volunteers

All staff/volunteers receive regular Online Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- Online Safety training is made available to staff. An audit of the online safety training needs of all staff is carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements

- This Online safety Policy and its updates are presented to and discussed by staff in staff meetings
- The Online Safety Coordinator/ DSL provides advice / guidance / training as required to individuals

All staff are familiar with the school policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school approved system including Microsoft TEAMS
- Safe use of the school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs/calendars and information available on the school website
- Capturing and storing photographs/videos/audio files on personal and school/academy owned devices
- Cyberbullying procedures
- Their role in providing Online safety/E-Safety education for pupils
- The need to keep personal information secure

All staff are reminded / updated about Online/E-Safety matters at least once a year.

Governors

Governors take part in Online Safety training / awareness sessions.

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / RMUnify/ DSPPB or other relevant organisation
- Participation in school training / information sessions for staff or parents
- Invitation to attend lessons, assemblies and focus days

Filtering and Monitoring

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

Filtering

RMUnify filtering is provided by Smoothwall. The IWF (Internet Watch Foundation) list and the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office", is integrated into the Smoothwall database.

Web filtering policies are applied based on:
"who" (user or user group from a directory),
"what" (type of content),
"where" (client address – either host, subnet or range),
"when" (time period) in a filtering policy table that is processed from top-down

Monitoring

RMUnify's monitoring solution is provided by Smoothwall. Smoothwall's detection technology monitors imagery, words and contextual phrases, during online and offline activity, to identify behaviour which may represent a safeguarding risk or breach of acceptable use policies.

School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the AUA's

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users

Harmful keywords

As part of filtering and monitoring security settings there are some words that are blocked by the system. There are various categories like:

- pertaining to white supremacy

- pertaining to radicalisation

- pertaining to drug and substance abuse

- pertaining to pornography and explicit content

- pertaining to mental illness

- pertaining to violence and abuse

- pertaining to discrimination

- pertaining to bullying and cyberbullying

- pertaining to piracy and hacking

All users will have clearly defined access rights to school ICT systems

- All users will be provided with a username and password. In some cases, classes may have group log-ons and passwords where cognitive ability determines.
- Users will be required to change their password regularly, prompted by the online system through RM.

- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by RMUnify. The school can provide enhanced user-level filtering through the use of Smoothwall filtering or a MDMs (Managed Mobile Device system)
- The school manages and updates filtering issues through the management console
- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Co-Ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety committee.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential online safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access to "guests" (e.g. trainee teachers, visitors) onto the school/academy system. This is auditable. This is line with the procedure for all permanent members of staff and includes the signing of the relevant AUA.
- A guardianship document is signed before school/academy owned equipment leaves the premises. This clearly outlines the user's responsibilities – See appendix 4
- An agreed procedure is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school owned laptops and other portable devices that may be used out of the school. This is documented in accordance with the guardianship loan form.
- The school does not permit the use of unencrypted removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured
- The school has responsibility for ensuring files and applications accessed via CC4 Anywhere or a similar application, comply with information and data security practices.

Responsibilities

Governing Body

Have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met .

To do this they:

- should identify and assign a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers

Senior Leadership Team

Responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Staff Members

Responsible for:

- Identifying the risks for pupils
- Take active part in training and CPD
- Monitor pupils' internet access
- Report any issues or incidents to Online Safety Coordinator

Staff should report to Online Safety Coordinator if:

- They see or suspect inappropriate content has been accessed
- They suspect inappropriate content can be accessed
- They are using teaching materials that may cause a spike in logs
- Filtering restrictions are perceived to be unreasonable
- Misspelling or abbreviations allow access to inappropriate content
- They suspect the system is being abused or is failing to protect users

1. Specific Online Safety Issues

Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI

Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to such incident in line with Safeguarding and Behaviour for Life and Learning policies.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Anti-radicalisation Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Anti-Radicalisation Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.

- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

2. Use of Smart Technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behavioural Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

3. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

10. Curriculum

Online/E-Safety is a focus in all areas of the curriculum. The new Computing Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy is taught. Staff will re-enforce Online safety/E-Safety messages in the use of ICT across the curriculum and during Computing lessons. This is delivered at a level appropriate for the cognitive development and understanding of each pupil. Where appropriate pupils are taught using adopted Sheffield SEND Computing SoW.

- In lessons, where internet use is planned, pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches.
- The school provides opportunities within a range of curriculum areas to teach about Online Safety
- The school teaches 'Digital Literacy' as part of the 'Computing' programme of study. This is incorporated into the schools PHSCE curriculum.
- 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 can request that the network manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying, Sexting and Radicalisation and know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

4. Use of digital and video images

When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the storing, sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils **are not** permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Care is taken when capturing digital / video images, ensuring pupils are appropriately dressed and that they 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
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website or on an official school social networking application – See appendix 5
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Further guidance can be found at

https://dudleysafeguarding.org.uk/children/parents-and-carers/online-safety-and-use-of-images/

5. Data Protection

The school has a Data Protection Policy that meets statutory guidance.

By following and maintaining strict safeguards and controls in line with General Data Protection Regulation from May 2018, **Pens Meadow School** and the School Governing Body will:

- Acknowledge the rights of individuals to whom personal data relate, and ensure that these rights may be exercised in accordance with Data Protection Law;
- Ensure that individuals are fully informed about the collection and use of personal data through the publication of the school's Privacy Notice;
- Collect and process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Ensure that adequate steps are taken to ensure the accuracy and currency of data;
- Ensure that for all personal data, appropriate security measures are taken – both technically and organisationally – to protect against damage, loss or abuse;
- Ensure that the movement of personal data is done in a lawful way – both inside and outside the organisation and that suitable safeguards exist at all times.

Staff are aware of the 'School Information Security Policy'. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices, at the school and home, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Please refer to School Information Security Policy for further guidance.

6. Communications

When using communication technologies, the school/academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in the school or on school systems e.g. by remote access from home
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal** email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Pupils are provided with individual/group school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be secured in the office.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device

7. Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school has a policy that sets out clear guidance for staff to manage risk and behaviour online.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety/online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

8. Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation May 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure online safety is a key focus.

However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to Dudley Children Front Door

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

- Complaints related to child protection are dealt with in accordance with school, DSCPPB child protection procedures.

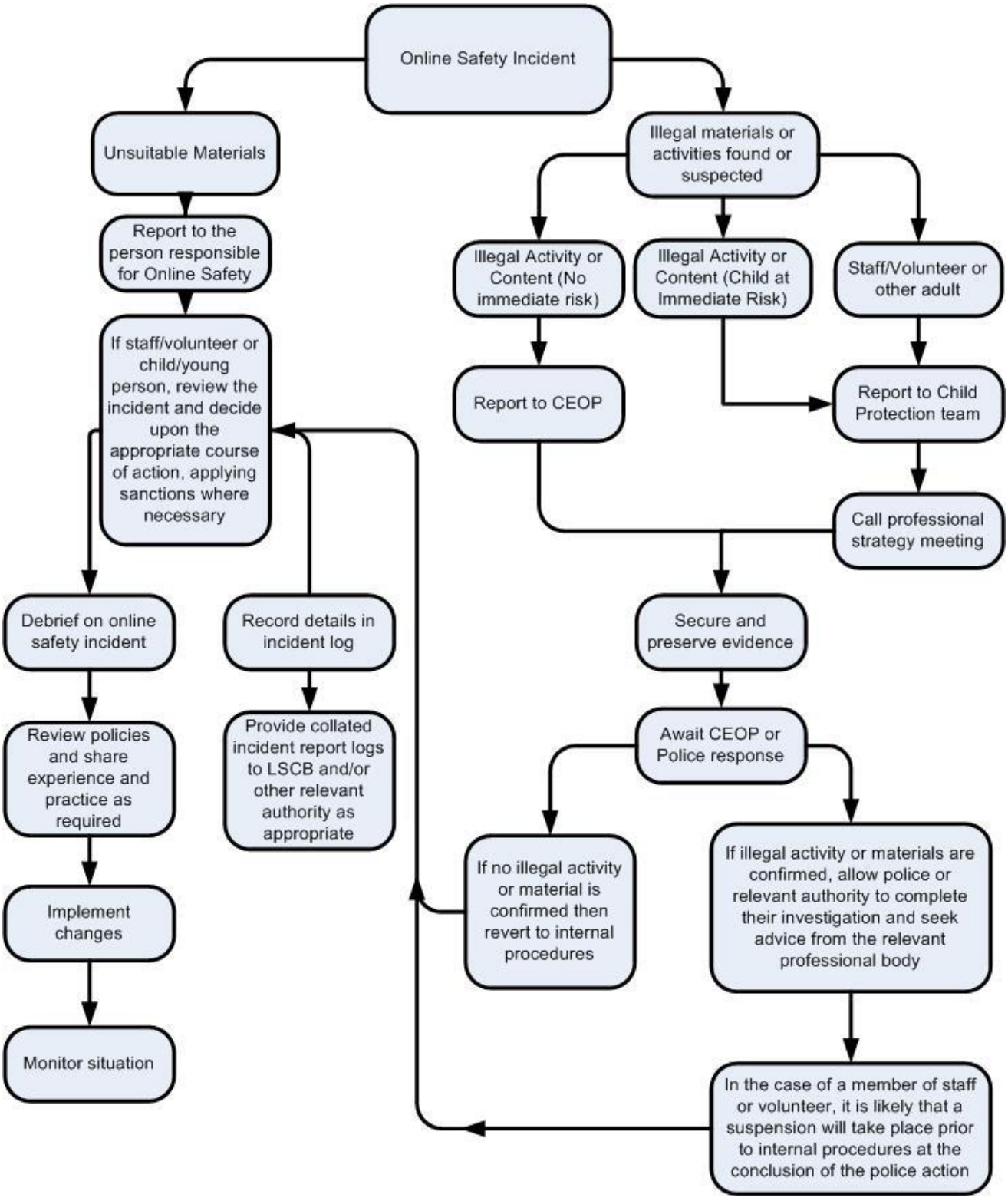
There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

This E-Safety Guidance and Policy has been written with references to the following sources of information:

Dudley LA, Hertfordshire E-Safety Policy, Kent e-Safety Policies, Information and Guidance, South West Grid For Learning- Online Safety School template Policies

This policy will be reviewed on an annual basis.

Appendix 1- Online safety response



Appendix 2- Online safety tools available on the RMUnify network

E-Safety tool	Type	Availability	Where	Details
Smoothwall filtering	Web filtering	Provided as part of RMUnify	All network connected devices within RMUnify	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of RMUnify	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUA	Awareness raising	Part of CC4- needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
Smoothwall	Monitoring software- *licenses available on Windows, Apple Mac*	Available to all schools	All school Windows 11 desktops and networked laptops and Apple Mac networks	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Reports are sent to designated staff in school

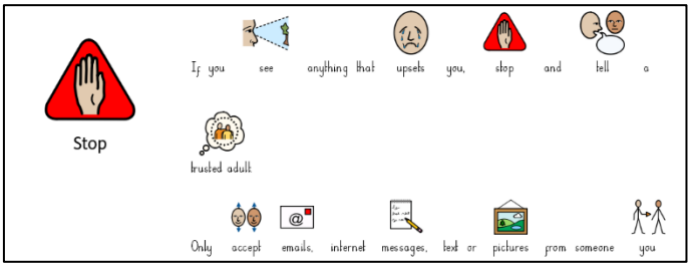
Email	Filtering and list control	Provided as part of RMUnify	Office 365	Allows schools to restrict where email is sent from/to
RM Password Plus	Safe practice	Provided as part of RMUnify3	All CC5 stations	A password management tool that enforces password rules of complexity and length for different users

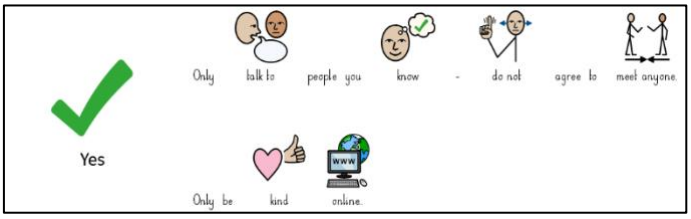
Appendix 3- Pupil AUA

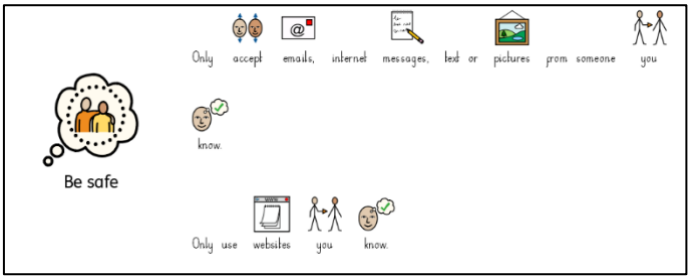
Pens Meadow School

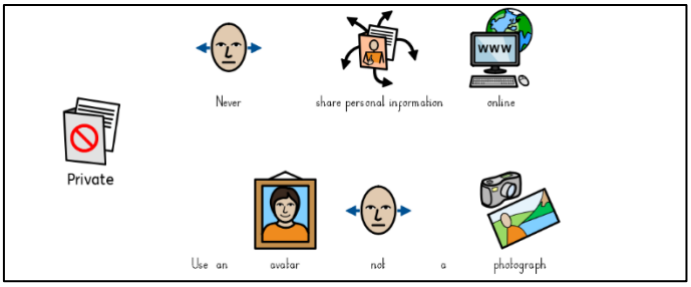
Rules for Responsible Internet Use - Pupils

At Pens Meadow we encourage the safe use of digital technology including the use of the internet to support learning. In order to safeguard everyone involved we ask pupils to follow these rules.









I agree to use the internet safely, thinking about what I do, the type of words I use and how I behave online. I know that if I see or read something that makes me feel uncomfortable, then I will tell a trusted adult.

Head/Deputy Head Teacher Signed: Date:

Student Signed: Date:

Appendix 4

Pens Meadow School

Staff Acceptable Use Agreement

Rules for Responsible Internet use

This policy applies to all adult users of the school's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of RMUnify, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and

- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply: -

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia

- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter

When using school approved social networking sites the following statements apply: -

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from pupils. The legal age for Pupils to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @pens-meadow.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the General Data Protection Regulation May 2018. Schools are defined in law as separate legal entities for the purposes of complying with the General Data Protection Regulation May 2018. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must: -

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the General Data Protection Regulation May 2018 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:……

PRINT NAME……

Dated: ……..

Appendix 5

Pens Meadow School

Community User- Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all community users of the school's systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of RMUnify, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.
- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:…… PRINT NAME……

Dated: ……

Appendix 6: Guardianship Loan Form

Member of staff	

has permission to loan and is guardian of the following item of ICT equipment:

Asset ID	Item	Serial No	Start date	Return/ Disposal date

Whilst the above item is in your care, the school will expect you to take full personal responsibility for the safe custody of it and to follow the guidelines below:-

- I will ensure the mobile device is secured or locked away when not in use;
- I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives / memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure that data remains confidential and secure;
- Any personal data stored on the device will be encrypted if appropriate and removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Signed:		**Date:**	

Person Authorising Loan

Name		**Job Title**	
Signed:		**Date:**	