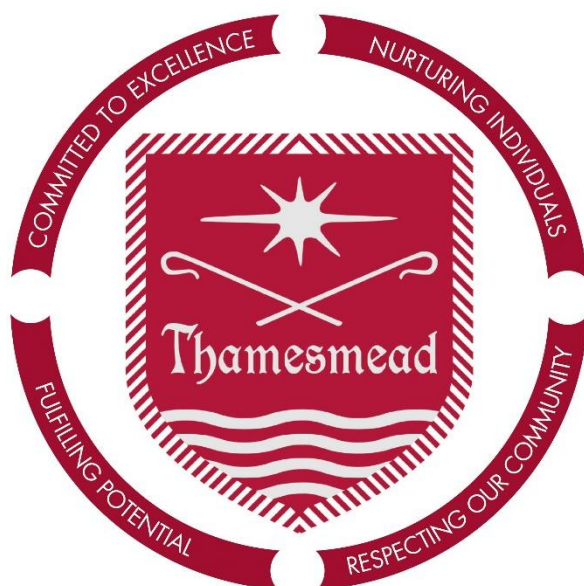


Thamesmead School



Online Safety Policy

Person Responsible	DSL
Review Period	Every 2 Years
Committee	PDB&W Committee
Date of Review	Summer 2026
Date of next Review	Autumn 2028

Contents

1. Aims and Principles	3
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	4
4. Educating students about online safety	6
5. Educating parents about online safety	7
6. Cyber-bullying, image-based abuse and AI misuse.....	7
7. Acceptable use of the internet in school	11
8. Students using mobile devices in school	11
9. Staff using work devices outside school	11
If staff have any concerns over the security of their device, they must seek advice from the Network Manager.....	12
Staff should also be alert to potential risks of data breaches when using portable devices, and must immediately report any suspected breach to the DSL and Data Protection Officer.	12
10. How the school will respond to issues of misuse	12
11. Training	12
11.2 Students.....	13
12. Monitoring arrangements.....	13
13. Links with other policies	14
Appendix 1: KS2, KS3 and KS4 acceptable use agreement (students and their parents/carers)	15
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors).....	17

1. Aims and Principles

Principles:

This policy applies to the whole school community. Online safety is the responsibility of everyone – not just computer science teachers, DSLs or technical staff. Whole-school approaches to online safety are far more effective than lessons alone, encompassing the school's ethos, environment, and partnerships with families and the community. The emphasis should be on developing knowledge, behaviours and critical thinking, not simply following a list of rules.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as “mobile phones”)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk:

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images, online bullying, and the misuse or AI manipulation of images to bully, harass, blackmail or create abusive content.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education.
- Searching, screening and confiscation
- [Filtering and monitoring standards for schools and colleges](#)

This policy also takes account of UKCIS and UK Safer Internet Centre guidance, including guidance on sharing nudes and semi-nudes, responding to online safety incidents, and protecting children

and young people's images from AI manipulation, abuse, blackmail and AI-generated child sexual abuse material.

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

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure students are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and networks, and will regularly review their effectiveness.

The board will review the DfE filtering and monitoring standards (2024), and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

- Having effective monitoring strategies in place that meet their safeguarding needs.

The governing board will ensure that, where necessary, teaching about safeguarding (including online safety) is adapted for vulnerable students, victims of abuse, and students with SEND, recognising that a “one size fits all” approach may not be appropriate.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

They are also responsible for ensuring staff receive regular updates, that incidents are properly logged, and that students receive age-appropriate online safety education.

3.3 The designated safeguarding lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Providing governors with assurance that filtering and monitoring systems are effective and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school’s child protection policy
- Responding to safeguarding concerns identified through filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with external agencies or services when required
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Maintaining secure filtering and monitoring systems that meet DfE 2024 standards
- Ensuring all safety mechanisms are updated regularly and reviewed at least annually
- Conducting a full security check and monitoring the school’s ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Logging any online safety incidents in coordination with the DSL

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy and implementing it consistently
- Agreeing and adhering to the acceptable use terms for ICT systems (Appendix 3)
- Ensuring students follow the acceptable use agreements (Appendices 1 and 2)
- Reporting any online safety concerns or breaches to the DSL
- Responding appropriately to all reports and concerns of online abuse, including sexual harassment or violence
- Understanding that the DSL oversees filtering and monitoring systems, and knowing how to report any failure of those systems
- Applying the school's image-security expectations when taking, storing, displaying or sharing images of pupils, including checking consent, avoiding unnecessary identifiable information, using safer image choices where appropriate, applying access controls and reporting any concern about image misuse, alteration or AI manipulation to the DSL.

3.6 Parents/carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum and through assemblies, tutor sessions and themed events:

- [Relationships and sex education and health education](#) in secondary schools.

In **Key Stage 3**, students will be taught to:

- Use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns and access support

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including the permanence of shared material
- The impact of viewing harmful content (e.g. pornography, self-harm, extremism)
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- The effects of online comparison, body image pressure, online gambling, and targeted advertising
- How online consent operates and how it can be withdrawn

Online safety teaching will be adapted for vulnerable students and those with SEND to ensure accessibility and understanding.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety through letters, the school website and other communications home.

Online safety will also be discussed at parents' evenings and information events.

This policy will be available to all parents on request and published online.

Parents will be informed about:

- The school's filtering and monitoring systems
- What students are expected to do online, including which platforms and learning tools they may access
- Who from the school (if anyone) they might communicate with online

If parents have any queries or concerns about online safety, they should raise them with the headteacher and/or DSL in the first instance.

6. Cyber-bullying, image-based abuse and AI misuse

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or

group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

The school will:

- Ensure students understand what cyber-bullying is and how to report it
- Encourage students to report incidents, including those where they are witnesses rather than victims
- Actively discuss cyber-bullying in assemblies and lessons (e.g. citizenship, PSHE, computer science)
- Provide training for staff, governors and volunteers on recognising, responding to and supporting students affected by online bullying
- Share information with parents about recognising signs of cyber-bullying and how to respond

When an incident occurs:

- The school will follow its behaviour policy and, where relevant, the child protection policy
- If illegal or harmful material has been shared, the school will take all reasonable steps to contain it
- The DSL will decide whether police involvement is necessary and will liaise with external agencies if required

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from SLT
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

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

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

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

If inappropriate material is found on the device, it is up to the Safeguarding Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools such as ChatGPT and Google Gemini are now widely available. While they can support learning, they also present safeguarding risks.

The school recognises that AI can be misused to bully others (for example, through deepfakes or AI-

generated explicit material).

Any such use will be treated seriously in line with the behaviour policy.

Staff must carry out a risk assessment before introducing new AI tools into teaching or administrative processes. Any use of AI will follow the principles of safeguarding, data protection and fairness.

6.5 Use of pupil images and prevention of AI image manipulation, abuse and AI-CSAM

Thamesmead School recognises that photographs and videos of pupils can support learning, celebration, communication and the wider life of the school. However, the school also recognises that images of children and young people can be misused, copied, altered or manipulated, including through artificial intelligence tools. This may include the creation of deepfakes, non-consensual altered images, blackmail material or AI-generated child sexual abuse material. The use of pupil images will therefore be managed as both an online safety and safeguarding matter.

When using, storing, displaying or sharing images of pupils, staff must take proportionate steps to reduce the risk of misuse. These steps include:

- Ensuring that images do not contain unnecessary identifiable information that could be used to harm, locate, target or blackmail an individual. In particular, full names and other personal details must not be displayed or shared alongside pupil images unless there is a clear, approved and lawful reason to do so.
- Considering whether images of pupils are needed at all, or whether the same purpose can be achieved through images without identifiable faces, such as images of work, activities, displays, equipment, over-the-shoulder shots, group shots from a distance, blurred images or images where pupils are not directly facing the camera.
- Using imagery that is harder to misuse or abuse where appropriate, including photographs taken from a distance, images taken from behind or over the shoulder, images with reduced detail, blurred images, lower-resolution images or images focused on the activity rather than the individual pupil.
- Applying appropriate privacy settings and access controls to limit who can view, download, store or share images. This applies to images used on social media, websites, internal platforms, cloud storage, shared drives, newsletters, displays and any other place where images are stored or shared.
- Removing metadata, including EXIF data, from images before publication or wider sharing where possible. Metadata can reveal location, device details, dates or timestamps and may unintentionally disclose routines, schedules or patterns of attendance.
- Ensuring that consent and image-use preferences are checked before images are used, and that particular care is taken for pupils who may be vulnerable or subject to safeguarding, custody, legal, anonymity or other protection concerns.
- Avoiding the unnecessary use of pupil images in public-facing or visitor-accessible areas where the image could be photographed or copied, unless the use has been risk-assessed and is considered appropriate.

- Reviewing and removing images that are out of date, no longer needed, no longer reflect current consent, or feature pupils who are no longer members of the school community, where continued use is not necessary or appropriate.
- Embedding image-security awareness into staff training, safeguarding practice, communications practice and relevant school policies.

Where staff become aware that a pupil image has been misused, altered, shared without consent, used to threaten or blackmail, or used or suspected to have been used to create sexualised or abusive content, they must report this immediately to the DSL or a member of the safeguarding team. Staff must not further share the image or related material. Where material may constitute evidence of an offence, staff must not delete it without advice from the DSL, senior leadership or the police. The school will prioritise the pupil's safety, dignity and emotional wellbeing, follow safeguarding procedures, consider whether the matter should be reported to the police, and take steps to remove or restrict access to the original image where appropriate.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Filtering systems will restrict access to harmful or inappropriate content without unreasonably impacting teaching and learning.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during the school day. This includes Smart devices, such as Smart watches, mobile phones and any such-related technology.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

Staff should also be alert to potential risks of data breaches when using portable devices, and must immediately report any suspected breach to the DSL and Data Protection Officer.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on acceptable use of technology. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

All incidents of misuse will be recorded by the DSL or ICT Manager, including any actions taken and lessons learned. These records will be reviewed regularly to identify patterns or recurring risks.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, online sexual harassment, grooming and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sexualised or exploitative content generated by AI or deepfakes
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Image-based abuse and AI image manipulation, including how student images may be copied, altered, misused, used for blackmail or used to create AI-generated child sexual abuse material.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL/DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Students

Students will receive age-appropriate training on digital resilience and safe internet use, including:

- Recognising phishing and social engineering tactics
- Password creation and multi-factor authentication
- How to identify and report cyber incidents or personal data breaches
- How AI-generated content and misinformation can be misleading or harmful
- Reporting online harm through both school and national channels (e.g. Report Harmful Content, CEOP, Childline)

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety that are flagged by the Monitoring system in school, Classroom Cloud.

These logs will be regularly reviewed to identify trends, training needs or recurring concerns.

This policy will be reviewed every 2 years by the DSL with responsibility for Online Safety. At every review, the policy will be shared with the governing board.

An annual risk assessment will also be undertaken to ensure the policy and filtering/monitoring provisions remain effective and reflect emerging technologies and risks.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Relationships and Sex Education (RSE) Policy

Appendix 1: KS2, KS3 and KS4 acceptable use agreement **(students and their parents/carers)**

THAMESMEAD SCHOOL - ICT ACCEPTABLE USE POLICY

This policy is to protect all parties, the school, its staff and its students. Please read this carefully. Any violations of this agreement will result in access to the System being revoked and the application of further sanctions deemed appropriate by School staff.

The School Computer System is owned by the school and is available to students to enhance their learning, and for staff to assist their professional activities. The system includes ALL PC and laptop hardware and software, network switches, cabling and data socket outlets, and all cabinets, desks, tables and trolleys where these are installed.

The School reserves the right to examine any files that are held on the computer system, monitor websites visited, intercept e-mails and delete files as appropriate, in circumstances where it is deemed that there has been inappropriate, unauthorised or unlawful use of the system. Users must:

- Treat all computer equipment with respect
- Access the system using only their own personal login and password
- Keep their password secret and inform staff if they suspect someone else knows it
- Save all files in their own user area
- Report any faults to an appropriate member of staff
- Always log off at the end of a computer session or lock screen if you are temporarily away from your work station
- Print responsibly – use print preview to check number of pages
- Use the internet appropriately according to students learning needs and staff professional activity
- Check all files created outside school for viruses
- Maintain correct language in e-mails

Users must NOT:

- Alter or delete settings on school computer equipment
- Introduce unauthorised software onto school computers or network
- Eat or drink on or around computers
- Use school computer equipment for playing games other than when allowed to by staff
- Use school computers to access Bulletin Boards, Chatrooms, Forums and Instant Messaging systems

E-mail

The sending or receiving of any email containing inappropriate material is strictly forbidden. This material includes pornography, unethical or illegal requests, racism, sexism, bad or inappropriate language and anything likely to cause offence. Disciplinary action will be taken in all cases. Large volume email sending (spamming) is also banned.

Vandalism

Vandalism of the School Computer System is defined as any attempt to harm or destroy any item of system equipment or data or that of another user. This includes, but not limited to, theft, virus creation or replication, wilful damage, deletion or modification of system or other user data and defacing system hardware. Anybody caught vandalising the system will have their access revoked and will face further punishment including paying for the damage caused.

User Areas

User areas are for the storage of coursework and classwork only. All non classwork related material, such as audio/video files, .exes (games etc) and applications is banned. Music content is NOT allowed to be stored on user areas. It takes up valuable space and is also illegal as it constitutes an infringement of copyright. User areas will be scanned periodically and any such files found will be deleted. Any user found to be copying music will face disciplinary action and could have their access revoked.

Miscellaneous

Any students found to be posting any material on public systems outside of school that bring Thamesmead School or its staff into disrepute, or is in any way deemed to be defamatory or offensive will face disciplinary action by School staff. The matter may also be passed to the Police if the situation warrants it.

Students full names and other details will never be stored together with their pictures on any publicly accessible area. This includes the school website and is to protect students.

Computer Misuse Act 1990

Thamesmead School is covered by this act. It recognises three key offences –

1. Unauthorised access to computer material
2. Unauthorised modification of computer material
3. Unauthorised access with intent to commit or facilitate further offences

If the School deems that any of the above offences have occurred, it may notify the Police. Penalties include fines AND imprisonment.

The School operates an online real-time scanning system which scans students desktops and reports inappropriate system use to ICT Network Support staff who pass the details onto the School Leadership Team for further action.

I agree to comply with the school's ICT Acceptable Use Policy.

Student's Signature..... Date.....

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

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

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date: