GATEHOUSE SCHOOL

# Online Safety Policy

| | |
|---|---|
| **Reviewed by:** | Pauline Moisy (DSL)<br>Fiona Tighe (DDSL)<br>Tom Sheldon (Head of KS1 and KS2)<br>Robert Conway (Computing Teacher) |
| **Approved by:** | Governors |
| **Date Approved:** | September 2025 |
| **Next Review:** | June 2026 |

# 0. Document Control

The table below contains the changes made between the different final editions of this document set for approval. This is to help provide information to those reviewing and approving the document of the changes being made.

| Document Edition | Section | Details of change |
|---|---|---|
| September 2025 | All Sections | Full policy review, formatting. Updates from KCSIE 2025. |

# 1. Scope of the Policy

Gatehouse School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

**Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

**Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

**Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

**Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Contractors and visitors accessing the school's network or systems must comply with this policy and the Staff Acceptable Use Agreement.

This policy should be read in conjunction with the Safeguarding Policy, Computing Policy, Data Protection (GDPR) Policy, Staff Code of Conduct, Digital Images Policy and Mobile Device Policy.

---

# 2. Roles and Responsibilities

## Governing Board / School Committee

The School Committee is responsible for:
Reviewing this policy on an annual basis.  Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers. Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

# Headteacher

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated. Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the ICT technicians and Senior Leaders to conduct termly light-touch reviews of this policy.
- Working Senior Leaders, to update this policy on an annual basis.
- Taking the lead responsibility for online safety in the school.
- 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.
- Reporting to the governing board about online safety on a termly basis.

# DSL

At Gatehouse School, the DSL is the Head of Pastoral Care, however some responsibilities may be delegated to deputy DSL's. These responsibilities include:

- 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, e.g. the SENCO and ICT technicians.
- 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.
- 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.
- Working with the ICT technicians and Senior Leaders to conduct termly light-touch reviews of this policy.

# ICT Technician

The ICT Technician is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher and DSL.
- Ensuring that the school's filtering and monitoring systems are reviewed, maintained, and updated in line with the **DfE Filtering and Monitoring Standards (2024)**.
- Collaborating with the DSL and Headteacher to investigate any online safety or cyber-security incidents recorded on CPOMS.
- Working with the Headteacher and DSL to conduct **half-termly light-touch reviews** of this policy, assessing system effectiveness and identifying areas for improvement.
- Keeping accurate records of system checks, supplier assurances, and configuration updates for audit and governor review.

## Staff

Staff are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to. Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology. Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

## Parents

Parents play an essential role in supporting the school's approach to online safety and digital responsibility. Gatehouse School recognises that a strong partnership between home and school helps to ensure that pupils use technology safely, respectfully, and responsibly both in and out of school.

Parents are encouraged to:

- Support the school's aims to promote safe, responsible, and positive use of technology.
- Read, discuss, and sign the **Pupil Acceptable Use Agreement** with their child, ensuring that its expectations are understood and upheld at home.
- Reinforce online safety messages provided by the school, including the importance of privacy, respect, and appropriate sharing of digital images and information.
- Monitor and guide their child's online activity outside of school, using appropriate parental controls, supervision, and discussion to encourage balanced, responsible use.
- Seek advice or support from school staff if they have concerns about their child's online behaviour, wellbeing, or digital footprint.

- Report any online safety incidents or concerns that involve pupils, whether occurring in or out of school, so that the school can respond appropriately in line with this policy.

The school will continue to provide parents with information, training opportunities, and regular updates to support them in promoting online safety and digital wellbeing at home.

---

# 3. Managing Online Safety

All staff recognise that technology is now a significant factor in many safeguarding and wellbeing concerns affecting children and young people. Risks may include exposure to harmful content, online bullying, exploitation, grooming, misinformation, and issues linked to screen time or digital wellbeing.

## 3.1 Leadership and Accountability

- The **Designated Safeguarding Lead (DSL)** holds overall responsibility for the school's approach to online safety, supported by the **Deputy DSL**, **Headteacher**, and **ICT Technician**.
- The DSL ensures that robust procedures are in place to identify, record and respond to online concerns, and liaises with the police, the LADO, or children's social-care services when incidents involve actual or suspected harm.
- The **Headteacher** ensures that online-safety measures are implemented across all school operations and that staff are appropriately trained.
- The **ICT Technician** implements and maintains technical safeguards (filtering, monitoring, cyber-security) and collaborates with the DSL to review system alerts and update controls as needed.

## 3.2 Whole-School Integration

Online safety is embedded throughout the school's culture and daily practice:

### 3.21 Training and Updates

- All staff and governors receive annual online-safety and cyber-security training; updates are issued mid-year or when new risks emerge.
- Staff receive periodic bulletins and email alerts summarising new threats, case studies, or legislation changes.

### 3.22 Curriculum Integration

- Online safety is explicitly taught through the **computing** and **PSHE/RHE** curricula and reinforced across subjects such as English and humanities.
- Lessons cover privacy, respectful communication, misinformation, ethical use of AI, and maintaining a healthy online/offline balance.

### 3.23 Assemblies and Events

- Assemblies are held **each term** to reinforce safe-use messages, celebrate positive digital behaviour, and remind pupils of reporting routes.
- The school participates annually in **Safer Internet Day** and other national initiatives.

### 3.24 Filtering and Monitoring Oversight

- Technical systems are reviewed **termly** by the DSL and ICT Technician in line with the DfE Filtering and Monitoring Standards (2024).
- Logs and review notes are retained for governor scrutiny.

### 3.25 Parental Engagement

- Parents receive annual workshops and ongoing guidance to promote consistent messages at home.

## 3.3 Incident Response

All online-safety incidents or concerns are reported immediately to the DSL and logged on **CPOMS**. The DSL, ICT technician and headteacher jointly investigate, take appropriate safeguarding or disciplinary action, and record outcomes and learning points.

---

# 4. Handling Online Safety Concerns

Any disclosures made by pupils to staff about online abuse, harassment or exploitation — whether they are the victim or disclosing on behalf of another child — will be handled in accordance with the **Child Protection and Safeguarding Policy** and the school's statutory duties under *Keeping Children Safe in Education (2025).*

Staff understand that **technology is a common pathway for child-on-child abuse** and that harmful online sexual behaviour can occur on a continuum from curiosity or poor decision-making through to coercive or abusive behaviour. Early identification and proportionate intervention can prevent escalation.

Staff also recognise that pupils displaying such behaviour are often **victims of abuse themselves** and must receive appropriate support alongside any necessary sanctions.

## 4.1 Responding to disclosures

- The victim's wishes will be considered carefully. The **DSL** will assess whether sharing details could increase the risk of harm or is required to protect the victim or others.
- Where it is necessary to share information, this will be done lawfully under **UK GDPR** using the *public-task* or *vital-interests* lawful basis.

- **Confidentiality will never be promised.** The DSL will explain what information must be shared, with whom, and why.
- If a report to Children's Social Care or the police is made **against the victim's wishes**, this will be managed sensitively, with ongoing communication and specialist support offered.
- The **DSL and Headteacher** will meet with parents/carers to explain safeguarding measures and agree continuing support for the child.

## 4.2 Recording and Investigation

- **All incidents are logged on CPOMS** within the same working day and include a record of actions, decisions, and outcomes.
- The **DSL**, **ICT Technician**, and **Headteacher** review logs to identify technical evidence, filtering breaches, or patterns of concern.

## 4.3 Concerns about staff or adults

- Concerns about a staff member's online behaviour are reported to the **Headteacher**, who will follow the *Managing Allegations Against Staff* and *Safeguarding* procedures.
- Where the concern relates to the **Headteacher**, the report is made directly to the **Chair of Governors**.
- Allegations that meet the harm threshold are referred to the **Local Authority Designated Officer (LADO)**.

## 4.4 Concerns about pupils

- Concerns about a pupil's online behaviour are reported immediately to the **DSL**, who investigates with relevant staff (e.g. Headteacher, ICT Technician) and acts in accordance with the **Behaviour**, **Safeguarding**, and **Child-on-Child Abuse** policies.
- Where illegal activity is suspected, the **Headteacher** contacts the police, following advice from the DSL.
- The school aims to **avoid unnecessary criminalisation** of pupils where behaviour stems from naivety or developmental curiosity (for example, consensual sharing of self-generated imagery). Each case is reviewed individually and sensitively.

## 4.5 Follow-up and learning

- The DSL ensures that victims receive appropriate pastoral or counselling support.
- Trends or recurring issues are analysed termly by the DSL and ICT Technician to inform staff training and curriculum updates.
- The **Safeguarding Link Governor** receives anonymised summaries of online-safety incidents as part of regular monitoring.

---

# 5. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text or online messages.

- Threatening or embarrassing pictures and video clips sent via mobile devices.
- Silent or abusive phone calls, or using the victim's phone or account to harass others.
- Threatening or bullying emails, possibly sent under a false name or pseudonym.
- Unpleasant or defamatory messages sent via instant messaging or gaming platforms.
- Unpleasant or harmful information posted to blogs, forums or social-media sites.
- Abuse between young people in intimate relationships online (e.g. non-consensual sharing of images).
- Discriminatory bullying online, including homophobia, racism, sexism, misogyny, ableism or transphobia.

The school recognises that certain pupils may be more at risk of online abuse and bullying, such as **pupils with SEND, pupils in care, LGBTQ+ pupils, and those experiencing social isolation.**

## 5.1 Prevention and Education

Gatehouse School promotes positive online behaviour and empathy through:

- Explicit teaching about respectful online communication and digital citizenship in **Computing** and **PSHE/RHE** lessons.
- Use of the **Gatehouse Champion Values**—Courage, Accountability, and Respect—to reinforce responsible online behaviour.
- **Termly assemblies** and **Safer Internet Day** participation to remind pupils how to report and support peers.
- Clear guidance on **how to block, report, or mute abusive content** on digital platforms.
- **Pupil voice and School Council initiatives** encouraging peer-led campaigns for kindness online.

## 5.2 Reporting and Response

- All allegations or reports of cyberbullying are treated seriously and investigated promptly.
- Pupils, staff and parents are encouraged to report incidents immediately to a trusted adult or directly to the **DSL**.
- Reports are recorded on **CPOMS** and reviewed by the **DSL**, **ICT Technician** and **Headteacher** to identify underlying causes or repeated behaviour.

- Technical evidence (e.g. screenshots or logs) is secured in accordance with **UK GDPR** and the **Data Protection Policy**.
- Where appropriate, the school will engage parents, social services, or police in line with the **Anti-Bullying Policy** and **Child Protection and Safeguarding Policy**.

## 5.3 Support for Pupils and Staff

- Victims receive tailored pastoral support, which may include restorative sessions, counselling or a mentor.
- Where pupils are perpetrators, a restorative approach is taken where appropriate, focusing on education and accountability.
- The school ensures staff are supported if they experience online abuse related to their professional role.

## 5.4 Monitoring and Review

- The **DSL** analyses CPOMS data termly to identify patterns of online abuse or vulnerability.
- Findings inform updates to curriculum content and staff training.

---

# 6. Child-On-Child Sexual Abuse and Harassment

All staff will be aware of the indicators of abuse, neglect, and exploitation, and understand that these harms can occur **both online and offline, inside and outside of school.** Staff recognise that pupils are often reluctant to report online sexual behaviours, especially if they involve sites or apps they know are inappropriate for their age.

Staff will remain alert to contextual indicators such as sudden anxiety, secrecy about online activity, peer withdrawal, or references to sexualised or coercive content.

**Examples of online harmful sexual behaviour include:**

- Threatening, facilitating or encouraging sexual violence.
- “Upskirting”, i.e. taking a photo under a person’s clothing without consent to view their genitals, buttocks or breasts.
- Sexualised online bullying, e.g. sharing sexual jokes or taunts.
- Unwanted or unsolicited sexual comments, messages, or images.
- Consensual or non-consensual sharing of sexualised or nude imagery.
- Abuse between young people in intimate relationships online (teenage relationship abuse).

## 6.1 Zero Tolerance and Culture

- The school promotes a **zero-tolerance approach** to all forms of sexually harassing or abusive behaviour, whether physical or online.
- Staff understand that minimising or dismissing such behaviour as “banter” or “just part of growing up” creates a culture that normalises abuse and silences victims.
- All incidents will be addressed immediately and proportionately to ensure that inappropriate behaviour is challenged and not repeated.

## 6.2 Legal Context

- Staff understand that creating, possessing, or distributing indecent images of anyone under 18 is a **criminal offence**, even if the image was self-generated or shared consensually.
- The **DSL** will determine the level of risk and decide, with the Headteacher, whether police involvement or Children’s Social Care referral is necessary.

## 6.3 Online and Social Media Context

- The school recognises that, following a disclosure or report, pupils involved may continue to interact on social media, leading to **further harassment or peer pressure**.
- The **DSL** and **ICT Technician** will monitor, where possible, any digital interactions related to the incident, ensuring swift intervention and pastoral support.
- Responses will align with the **Child-on-Child Abuse Policy**, **Social Media Policy**, and **Behaviour Policy**.

## 6.4 Reporting, Recording and Response

- All disclosures or concerns about online sexual harm are reported to the **DSL** and logged on **CPOMS** the same day.
- The **DSL** investigates in partnership with the **ICT Technician** (to preserve any technical evidence) and the **Headteacher**.
- Each case is assessed individually, taking into account the wishes of the victim, the level of risk, and the need for external referral.
- The **Safeguarding Link Governor** receives anonymised summaries of such incidents as part of termly safeguarding oversight.

## 6.5 Support for Victims and Pupils Involved

- Victims will be offered ongoing pastoral support, adjustments to routine where needed, and access to specialist services such as counselling or CAMHS.
- Pupils exhibiting harmful sexual behaviour are also supported through a **safeguarding and behaviour plan**, acknowledging that such behaviour often stems from unmet needs or trauma.

- Restorative and educational approaches will be used where appropriate to prevent reoccurrence.

## 6.6 Education and Prevention

- Teaching about consent, respectful relationships, body autonomy and online boundaries is delivered across the **Computing**, **PSHE/RHE**, and **assemblies** programmes.
- Pupils are taught how to report harmful behaviour safely and understand the school's processes for dealing with disclosures.
- The school regularly participates in **Safer Internet Day** and **Anti-Bullying Week**, using these events to reinforce the message that sexual harassment and abuse are never acceptable.

---

# 7. Grooming and Exploitation

Grooming is defined as a process whereby an adult – or, in some cases, another young person – builds a relationship of trust, secrecy, and emotional connection with a child with the intention of manipulating, exploiting, or abusing them.

Staff are aware that grooming frequently begins or progresses **online**, often through social media, gaming, messaging platforms, or live-streaming. Pupils who are being groomed are commonly reluctant to report what is happening due to manipulation, misplaced trust, affection, or fear.

## 7.1 Indicators of Online Grooming

The **DSL** ensures that online-safety training for staff includes recognising the signs of grooming, which may include (but are not limited to):

- Being secretive or defensive about time spent online or social media contacts.
- Having an older boyfriend/girlfriend, especially one not known to peers or family.
- Having unexplained gifts, money, or possessions such as clothing or devices.
- Increased anxiety, withdrawal, or preoccupation with online relationships.
- Sudden changes in friendship groups or behaviour.
- Using language, gestures, or knowledge that seem inappropriate for their age.
- Repeatedly missing school or disengaging from usual routines.

## 7.2 Types of Exploitation

- **Child Sexual Exploitation (CSE):** where children are coerced or enticed into sexual activity in exchange for attention, affection, gifts, or status.

- **Child Criminal Exploitation (CCE):** where children are manipulated or forced into criminal activity (e.g. county lines, drug distribution, financial fraud) often through online recruitment.

Staff understand that both forms of exploitation may overlap and that **technology is frequently used to initiate, maintain, and conceal exploitation.**

## 7.3 Reporting and Response

- Any concerns about possible grooming or exploitation are reported **immediately to the DSL** and logged on **CPOMS** the same day.
- The **DSL** assesses the concern, consults with the **Headteacher**, and decides whether to make a referral to the **police, Children's Social Care, or the Local Authority Designated Officer (LADO)**.
- The **ICT Technician** may assist in securing digital evidence (e.g. messages, logs, or screenshots) while maintaining confidentiality and data protection requirements.
- The school will never attempt to confront or contact an alleged groomer directly.

## 7.4 Education and Prevention

- Pupils are taught through the **Computing** and **PSHE/RHE** curricula about healthy online relationships, consent, manipulation tactics, and how to seek help.
- Lessons include recognising the tactics used by exploiters, such as flattery, gifts, or threats.
- The school promotes clear reporting routes and trusted adults pupils can approach.
- Parents are provided with guidance and signposted to resources (e.g. CEOP, Internet Matters, and Thinkuknow) to help them monitor and talk with their child about online risks.

## 7.5 Support for Victims

- The school provides pastoral support for any pupil identified as being at risk or involved in exploitation.
- Multi-agency working ensures wraparound support and ongoing risk reduction.
- Victims are treated with compassion and without judgement; safeguarding takes precedence over any disciplinary concerns.

---

# 8. Child Sexual Exploitation (CSE) and criminal exploitation (CCE)

Gatehouse School recognises that some forms of exploitation and abuse can begin or occur **online**, and that technology may be used to communicate with or manipulate children.

While explicit teaching about exploitation or grooming is not appropriate for primary pupils, staff are trained to understand that online contact can sometimes be used to influence, pressure, or harm children. Staff are alert to early indicators that a pupil may be at risk and know how to respond quickly and sensitively.

## 8.1 Staff Awareness and Responsibilities

- All staff receive safeguarding and online-safety training that includes awareness of potential online risks, including manipulation and exploitation.
- Staff are aware that children may not always recognise or disclose when something is unsafe online.
- Any concerns are reported **immediately to the DSL** and recorded on **CPOMS**.

## 8.2 Signs that May Raise Concern

Staff are alert to patterns such as:

- Secrecy around online activity.
  Receiving unexplained gifts, money, or technology.
- Increased contact with older individuals online.
- Anxiety, withdrawal, or changes in behaviour linked to internet use.

## 8.3 School Response

- The **DSL** assesses all concerns, working with the **Headteacher**, **ICT Technician**, and external agencies (where necessary) to ensure the pupil's safety.
- The school follows its **Child Protection and Safeguarding Policy** and cooperates with the **police** or **Children's Social Care** where required.
- Digital evidence (such as screenshots or messages) is handled securely under **UK GDPR** and **Data Protection Policy** principles.

## 8.4 Education and Prevention

- Pupils are taught, through the **Computing** and **PSHE/RHE** curricula, how to use technology safely, protect their personal information, and seek help from trusted adults.
- They learn about respect, healthy friendships, and making good choices online.
- Parents receive information and signposting to help them support children's online safety at home.

## 8.5 Support for Pupils

- Any pupil identified as vulnerable or at risk is supported through the school's pastoral and safeguarding systems.
- The DSL works closely with parents to ensure appropriate protection and ongoing monitoring.

# 9. Radicalisation

Radicalisation is the process by which an individual comes to support terrorism or extremist ideologies associated with terrorist groups. This process can happen gradually through **exposure to extremist content online**, or through **direct contact** with individuals who aim to influence or recruit young people.

Children may be targeted online by individuals or groups who appear caring, persuasive, or supportive, leading them to believe these people share their interests or values. Over time, such manipulation can make a child more willing to adopt harmful or extremist beliefs.

The school recognises that online platforms, including social media, gaming, livestreaming, and AI-generated content, can increase exposure to extremist narratives and persuasive techniques.

## 9.1 Staff Awareness and Training

- All staff receive regular **Prevent Duty** and **online-safety training** as part of the school's safeguarding programme.
- Staff are aware of the factors that may make some pupils more vulnerable to radicalisation, such as social isolation, curiosity about global events, or exposure to extremist materials.
- The school fosters resilience through the **Gatehouse Champion Values** of Courage, Respect, and Accountability, encouraging pupils to think critically and challenge harmful ideas safely.

  **Staff understand how radicalisation can intersect with other forms of online harm (e.g. grooming, hate speech, conspiracy theories).**

## 9.2 Recognising and Reporting Concerns

- Staff remain alert to changes in behaviour, increased secrecy, or expression of extreme views.
- Any concern about a pupil's exposure to extremist influence, content, or behaviour is reported **immediately to the DSL** and recorded on **CPOMS**.
- The **DSL** will manage the situation in accordance with the **Prevent Duty Policy**, consulting the **Headteacher** and, where necessary, making a **Prevent referral** or contacting **Children's Social Care** or the **police**.
- The school will engage parents where appropriate and provide supportive pastoral guidance for the pupil.

## 9.3 Education and Prevention

- Through the **PSHE/RHE** and **Computing** curricula, pupils learn about respect, inclusion, and responsible digital citizenship.
- Assemblies, circle time and class discussions encourage respect for difference, empathy, and democratic values.
- The school promotes awareness of how online platforms may be used to spread misinformation or extremist views, teaching children to question and verify online information.
- Pupils are taught how algorithms and AI-generated content can reinforce extremist messages, and how to seek balanced, trusted sources.
- The curriculum includes age-appropriate discussions on critical thinking, digital resilience, and reporting unsafe or extremist online content.

## 9.4 Community and Safeguarding Culture

Gatehouse School actively promotes a culture of tolerance and inclusion. Pupils are encouraged to develop a sense of belonging and to feel confident sharing their views within a safe environment. This proactive approach reduces vulnerability to extremist influence and supports pupils to make positive, respectful choices online and offline.

**The school works in partnership with external agencies, governors, and parents to monitor emerging online radicalisation risks and to ensure filtering/monitoring systems are effective in identifying extremist content.**

**Online safety, Prevent Duty and digital safeguarding are embedded across all policies, staff training, and whole-school safeguarding practice to ensure a coordinated and proactive approach.**

---

# 10. Online Wellbeing and Mental Health

Staff recognise that online activity—both in and outside of school—can significantly influence a pupil's emotional and mental wellbeing. Online interactions may have a **positive impact**, for example through creativity, collaboration and connection, but can also contribute to **anxiety, low self-esteem, isolation, or pressure to conform**.

The **DSL** ensures that staff receive regular training to:

- Understand the influence of social-media trends, digital communication styles, and online terminology.
- Recognise indicators that a pupil's mental health may be affected by their online experiences.
- Promote strategies for balance, healthy screen habits, and critical engagement with digital media.

All staff know how to respond when they have a concern:

- Immediate concerns about a pupil's wellbeing are recorded on **CPOMS** and referred to the **DSL**.
- The DSL coordinates support in line with the **Social, Emotional and Mental Health (SEMH) Policy**, working with parents, pastoral staff and external professionals as required.

The school promotes positive **digital wellbeing** through the **Computing** and **PSHE/RHE** curricula and the **Gatehouse Champion Values**, encouraging pupils to:

- manage screen time responsibly;
- reflect on their digital choices; and
- seek help from trusted adults when something online affects their feelings or confidence.

---

# 11. Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an **online hoax** is a deliberate falsehood designed to appear credible and provoke emotional or fearful reactions, often spread rapidly via social media or messaging platforms.

A **harmful online challenge** refers to digital challenges targeted at young people that encourage them to record or livestream themselves participating in a particular activity, often sharing footage across social platforms and urging others to do the same. While many challenges are harmless, a challenge becomes harmful when it:

- places participants at physical or psychological risk, or
- causes harm indirectly through online exposure or peer pressure.

## 11.1 Staff Responsibilities

- Staff are alert to rumours, viral content, or pupil discussions suggesting a harmful challenge or hoax may be circulating.
- Any suspicion or concern must be **reported immediately to the DSL** and **logged on CPOMS**.
- The **ICT Technician** supports the DSL by checking monitoring alerts and filtering data to determine whether harmful content is being accessed on school systems.

## 11.2 Assessment and Response

The **DSL** will carry out a **case-by-case risk assessment**, establishing:

- the scale and nature of the possible risk,
- the age group or pupils affected,
- whether the risk is local, regional, or national, and
- whether pupils have been directly exposed to or are discussing the content.

Where the harmful content appears to be circulating **locally**, the DSL consults with the **Local Authority** or **local police liaison** to agree a proportionate response and prevent wider spread.

Before any school communication or assembly takes place, the **Headteacher** will ensure that responses are:

- based on verified information from reliable sources (e.g. **UK Safer Internet Centre**, **National Online Safety**, **CEOP**, or **Childnet**);
- careful to **avoid unnecessarily amplifying** the content or frightening pupils;
- proportional to the age group and level of risk;
- supportive, focusing on reassurance and help-seeking; and
- aligned with the **Child Protection and Safeguarding Policy**.

## 11.3 Education and Prevention

- Through **Computing** and **PSHE/RHE** lessons, pupils learn to think critically about online content, check facts, and recognise sensationalised or manipulative material.
- The school promotes a culture of **digital resilience**, encouraging pupils to question sources, verify information, and speak to a trusted adult if something online causes worry.
- **Parents** are informed where appropriate and provided with guidance on monitoring devices, understanding viral trends, and supporting their child's online wellbeing.

## 11.4 Monitoring and Review

- The **DSL and ICT Technician** review filtering logs and monitoring alerts to ensure harmful content is blocked wherever possible.
- Incidents and responses are recorded on **CPOMS** and reviewed termly to identify emerging patterns or new digital threats.
- Lessons learned inform future **staff training** and **pupil education**.

---

# 12. Cyber Crime

## Definition

Cyber-crime refers to criminal activity committed using computers, digital devices or the internet. There are two principal categories:

- **Cyber-enabled crime:** offences that can occur offline but are facilitated or scaled up by technology, e.g. fraud, theft, the trade in illegal goods, or online exploitation.
- **Cyber-dependent crime:** offences that can only be carried out through digital systems, such as creating or distributing malware, unauthorised access (hacking), or "denial-of-service" attacks designed to disrupt networks.

## 12.1 Prevention and Early Identification

The school recognises that some pupils with a strong interest or aptitude in technology may, whether deliberately or inadvertently, engage in behaviour that breaches computer-misuse laws.

Staff are alert to early indicators such as:

- bypassing filters or attempting to access restricted systems;
- unusual interest in coding for intrusion or attack; or
- discussion of hacking or illegal downloads.

Where concerns arise, staff report them **immediately to the DSL** and record the issue on **CPOMS**.

The **DSL**, in consultation with the **ICT Technician** and **Headteacher**, will:

- assess intent and level of risk;
- consider a **referral to the Cyber Choices programme** (delivered by the National Crime Agency) to redirect technical interests into legitimate pathways; and
- provide pastoral and educational guidance to support positive engagement with computing.

## 12.2 Curriculum and Awareness

- Through the **Computing** curriculum, pupils learn to use technology **safely, responsibly, and lawfully**, including understanding digital footprints, copyright, and data ethics.
- **PSHE/RHE** lessons promote responsible digital behaviour and respect for others online.
- The school delivers a **cyber-awareness plan** for pupils and staff each year, covering password security, phishing, privacy, and safe device use.
- Technically-able pupils are encouraged to extend their interests through approved coding clubs, competitions, and STEM opportunities.

## 12.3 Staff Responsibilities and System Security

- Staff receive annual cyber-security training in line with the **DfE Cyber Security Standards (2024)**.
- The **ICT Technician** maintains up-to-date security controls, including encryption, multi-factor authentication, secure backups, and patch management.
- The **DSL** and **ICT Technician** meet termly to review filtering, monitoring and cyber-security logs, reporting outcomes to the **Safeguarding Link Governor**.
- The school's systems and protocols follow the **Cyber Security Policy** and **Data Protection Policy**.

---

# 13. Online Safety Training for Staff

The **DSL** ensures that all safeguarding and child-protection training for staff includes comprehensive coverage of **online safety**, in accordance with *Keeping Children Safe in Education (2025)* and the *DfE Filtering and Monitoring Standards (2024)*.

All staff are made aware that pupils can experience abuse, coercion, bullying, or exploitation **online as well as in person**, and that these often occur concurrently.

## 13.1 Training Content

Whole-staff training includes:

- How the internet and digital technologies can facilitate various forms of abuse (e.g. grooming, bullying, exploitation, radicalisation).
- Recognising the indicators of online harm and emotional distress linked to online activity.
- Understanding the school's **filtering and monitoring systems**, including how alerts are triaged and acted upon.
- The procedures for reporting online-safety concerns and logging incidents on **CPOMS**.
- Safe and professional conduct online, in line with the **Staff Code of Conduct** and **Acceptable Use Agreement**.
- Basic cyber-security awareness, including phishing, passwords, and data protection.

## 13.2 Role-Specific and Ongoing Training

- **DSL and Deputies** receive advanced training on managing online-safety incidents, reviewing system alerts, and liaising with law enforcement or external agencies.
- The **ICT Technician** completes training in line with the *DfE Cyber Security Standards (2024)* and supports the DSL in filtering and monitoring reviews.
- **Governors** receive annual updates to ensure they understand oversight responsibilities and can effectively scrutinise the school's online-safety provision.
- **Support staff and volunteers** are provided with practical guidance appropriate to their role, focusing on recognising and reporting early signs of online harm.
- Training materials and attendance are **recorded and monitored** by the DSL to ensure compliance and identify future CPD needs.

## 13.3 Continuous Development

- Online-safety and cyber-security awareness are refreshed **annually** for all staff and more frequently when new technologies, platforms, or threats emerge.
- Learning from any **CPOMS incidents** or **filtering alerts** is shared with staff to improve awareness and strengthen practice.

- Staff receive regular bulletins from the DSL highlighting key updates from organisations such as the **UK Safer Internet Centre**, **National Online Safety**, and **CEOP**.

---

# 14. Online Safety and the Curriculum

Online safety is embedded throughout the Gatehouse curriculum and underpins pupils' personal development as responsible digital citizens. It reflects the school's **Champion Values** of *Courage, Accountability, and Independence* by empowering pupils to make safe, informed and respectful choices online.

Online-safety learning is age-appropriate, progressive from EYFS – Year 6, and adapted for pupils' developmental stages.

**Subjects with explicit online-safety coverage include:**

- **Computing** – digital citizenship, privacy, coding ethics, online communication, AI awareness
- **PSHE/RHE** – relationships, consent, wellbeing, and respectful online behaviour
- **English** – media literacy, evaluating online information, and critical thinking
- **History & Humanities** – reliability of digital sources and bias in information
- **Assemblies and Cross-Curricular Events** – Safer Internet Day, Anti-Bullying Week, and Champion Values focus themes

**Knowledge and behaviours taught:**

- How to evaluate what they see online and recognise misinformation or "fake news" How to recognise persuasion and influence techniques, including in advertising and social media
- Acceptable and unacceptable online behaviour, including kindness and empathy online
- How to protect personal information and understand privacy settings
- How and when to seek help or report concerns
- How to balance screen time and maintain positive digital wellbeing
- Awareness of the ethical and responsible use of **AI and emerging technologies**
- Core media-literacy skills as outlined in the government's *Online Media Literacy Strategy*

Online-risk categories (content, contact, conduct, commerce) are considered when developing schemes of work so that lessons remain balanced and preventative.

## 14.1 Curriculum Development and Oversight

- The **DSL** is actively involved in designing and reviewing the online-safety curriculum to ensure alignment with safeguarding practice and current risks.
- Pupil voice activities inform planning, reflecting the platforms and technologies pupils actually use.
- The **SENCO** and **Designated Teacher for LAC** collaborate with class teachers to tailor content for pupils who may be more vulnerable to online harm, ensuring accessibility for pupils with SEND.
- Personalised or contextualised lessons are provided following any incident of online harm.

## 14.2 Teaching and Resources

- Class teachers review external materials before use to ensure suitability and factual accuracy.
- External visitors (e.g. police, online-safety educators) may support delivery where appropriate; their input is vetted and coordinated by the **Headteacher** and **DSL**.
- Before teaching a sensitive topic, the DSL advises on potential triggers and how to support pupils who may have experienced online abuse.
- Lessons are structured to maintain a **safe, non-judgemental environment**, encouraging openness and questions.

## 14.3 Responding to Disclosures and Concerns

- If a concern or disclosure arises during or after a lesson, staff follow the **Child Protection and Safeguarding Policy** and record the concern on **CPOMS** immediately.
- The DSL provides follow-up support and ensures any wider issues inform future teaching and staff training.

## 14.4 Monitoring and Evaluation

- The **DSL**, **Computing Lead** and **PSHE Lead** review curriculum coverage annually to ensure progression and relevance.
  Pupil surveys and lesson feedback are used to evaluate understanding and confidence.
- Findings are shared with the **Safeguarding Link Governor** and used to refine the curriculum and staff training.

---

# 15. The Use of Technology in the Classroom

A wide range of technology is used throughout lessons to enrich learning, develop digital literacy and prepare pupils for life in a connected world. This reflects Gatehouse's **Champion Values** of *Curiosity, Independence,* and *Accountability* through safe, creative and responsible use of digital tools.

## 15.1 Classroom Technology

Pupils and staff may use:

- **Desktop computers and Chromebooks** for research, publishing, and coding.
- **iPads and tablets** for interactive learning, media creation and accessibility support.
- **Interactive boards** and display technology for collaboration.
- **Digital cameras and microphones** for curriculum projects, creative media and performance recording.
- **The Gatehouse intranet and approved cloud platforms** (e.g. Google Workspace for Education) for communication and file sharing.
- **Email and online collaboration tools** for supervised educational communication.

## 15.2 Reviewing and Approving Digital Resources

Before using any new website, app, online platform, or AI-powered tool:

- Class teachers review and evaluate its **educational value, age-appropriateness, data-protection compliance, and accessibility**.
- The resource is checked for alignment with the **school's Filtering and Monitoring Policy**, ensuring it does not expose pupils to harmful or unmoderated content.
- Teachers ensure that all internet-derived materials are used in accordance with **copyright and licensing law**.
- AI-based platforms are used only for educational purposes and under teacher supervision; staff ensure that personal data is **never uploaded** to generative-AI tools.
- The **ICT Technician** maintains an approved-tools list and conducts periodic technical reviews with the **DSL** and **Headteacher**.

## 15.3 Supervision and Safeguarding

- Pupils are supervised appropriately for their age and ability whenever they access online content or communication tools.
- Teachers ensure that pupils understand how to use technology safely, including logging in securely, protecting passwords, and reporting any concerns.
- All digital use in class is covered by the **Acceptable Use Agreements (AUA)** for pupils and staff.
- Filtering and monitoring systems are active at all times on school devices and networks, with alerts reviewed by the **DSL** and **ICT Technician**.
- Any inappropriate use or safeguarding concern identified during lessons is reported immediately via **CPOMS**.

## 15.4 Extending Learning Beyond the Classroom

- When recommending or setting online tasks for home use, teachers ensure that platforms meet the same safety, privacy, and accessibility standards as those used in school.
- Parents are guided through the school newsletter and website on safe use of technology at home, including parental controls and digital wellbeing advice.

---

# 16. Smart Technology, Mobile Devices and Emerging Technologies

Gatehouse School recognises that smart technology—including mobile phones, tablets, smart watches, and AI-enabled devices—can have significant educational value when used safely and purposefully. However, the school also recognises that these technologies present safeguarding and wellbeing risks that must be managed carefully.

## 16.1 Education and Expectations

- Pupils are taught about the acceptable and responsible use of personal technology through **Computing, PSHE/RHE** and assemblies, promoting the **Champion Values** of *Respect, Accountability* and *Independence*.
- Pupils use technology in line with the **Pupil Acceptable Use Agreement (AUA)**, which sets clear expectations for device use, online behaviour and digital citizenship.
- Staff follow the **Staff ICT and Electronic Devices Policy** and **Staff AUA**, ensuring professional and appropriate use of all technology—whether school-owned or personal.
- The school educates pupils on managing the **4Cs of online risk** (content, contact, conduct and commerce), particularly in relation to mobile and smart-device use.

## 16.2 Supervision and Restrictions

- Pupils are **not permitted to use mobile phones or personal smart devices in the classroom** or during learning activities.
- Where necessary, the school may **ban or restrict the use of personal technology** on site.
- The school operates a **zero-tolerance approach** to the misuse of smart technology for bullying, harassment, sexting, trolling or viewing harmful content.
- All online-safety incidents and concerns about misuse are **recorded on CPOMS** and investigated by the **DSL** in collaboration with the **ICT Technician** and **Headteacher**.

## 16.3 Response and Support

- Misuse of smart technology is addressed in accordance with the **Behaviour Policy** and, where relevant, the **Child Protection and Safeguarding Policy**.
- Where misuse involves online harassment or illegal activity, the DSL will liaise with external agencies, including the police, as appropriate.
- The school responds with both **education and consequence**: assemblies, class discussions, and targeted interventions are used to reinforce appropriate use.
- The DSL and ICT Technician review any pattern of misuse to identify emerging trends and update staff and parents accordingly.

## 16.4 Monitoring and Emerging Technology

- The school remains informed about emerging platforms, devices, and risks (including **AI-driven chat, social-media trends, and wearable tech**).
- Filtering and monitoring systems are configured to identify high-risk content and alerts linked to mobile use when pupils connect to the school network.
- The **DSL and ICT Technician** review logs half-termly and adjust safeguards where required.
- Parents are regularly updated through newsletters and workshops on managing smart devices safely at home.

---

# 17. Working with Parents

Gatehouse School recognises that pupils' online experiences extend beyond school hours and networks. The school therefore works in **partnership with parents and carers** to help children stay safe online both at school and at home, reflecting our **Champion Values** of *Accountability, Respect,* and *Independence*.

Parents are provided with clear information about the school's approach to online safety, filtering, monitoring, and data protection, alongside their own vital role in supporting positive digital behaviour.

## 17.1 Acceptable Use and Communication

- At the start of each academic year, parents are sent a copy of the **Pupil Acceptable Use Agreement (AUA)** and are encouraged to review it with their child to ensure shared understanding.
- The school reinforces the message that online safety is a **shared responsibility** between school and home.
- Where a pupil is involved in an online-safety incident, the **DSL** will communicate sensitively and promptly with parents to agree a consistent approach to education and support.

## 17.2 Parental Awareness and Risks Discussed

Parents are made aware of the different ways children can be at risk online, including (but not limited to):

- **Child sexual abuse**, including grooming and exploitation.
- **Exposure to radicalising or extremist content.**
- **Sharing of indecent imagery** (e.g. sexting or peer-to-peer sharing).
- **Cyberbullying** and online harassment.
- **Exposure to age-inappropriate or harmful content**, including pornography, violence, or self-destructive behaviour.
- **Privacy and data misuse**, such as scams or identity theft.
- **Excessive screen time, online gaming, and digital wellbeing.**
- **AI-related risks**, such as misinformation, deepfakes, or unsafe use of generative-AI tools.

## 17.3 Supporting Parents to Keep Children Safe Online

Parents are supported with clear, practical advice on how to protect their children at home, including:

- Setting **age-appropriate parental controls** and privacy filters.
- Monitoring and discussing their child's online activity and screen time.
- Encouraging open conversations about online experiences and peer pressure.
- Using recommended resources from trusted organisations such as the **UK Safer Internet Centre**, **National Online Safety**, and **CEOP**.

## 17.4 Parental Engagement Activities

The school promotes ongoing parental engagement through:

- **Parents' Evenings** – highlighting online safety and digital wellbeing.
- **Dedicated Workshops** – covering topics such as social media, gaming, AI and privacy.
- **Termly Newsletters** and **Digital Safety Bulletins** – sharing tips, current risks, and guidance.
- **Website Updates** – providing quick access to up-to-date advice and recommended online resources.
- **Information Leaflets** sent home during national campaigns, e.g. *Safer Internet Day*.

The **DSL** and **ICT Technician** jointly oversee the creation and distribution of these communications, ensuring information is accurate, relevant, and accessible to all families.

## 17.5 Monitoring and Feedback

- Parents' feedback is actively sought to evaluate the effectiveness of the school's online-safety education.

- Outcomes are shared with the **Safeguarding Link Governor** and used to inform the Online Safety Action Plan.
- Parents are reminded that concerns about online safety or their child's digital behaviour can be raised directly with the **DSL** or through the school office at any time.

---

# 18. Internet Access

Access to the school's internet network is a privilege that supports teaching, learning, and communication.

## 18.1 Access and Authorisation

- Staff, pupils, governors, and visitors will only be granted access to the school's internet and network systems once they have read, understood, and signed the relevant **Acceptable Use Agreement (AUA)**.
- A record of authorised users is securely maintained in the **school office** and updated annually.
- All users must follow the **Data Protection Policy**, **Online Safety Policy**, and **Cyber Security Policy** when accessing or sharing information.

## 18.2 Use of the School Network

- All members of the school community are strongly encouraged to use the **school's filtered and monitored internet connection** instead of personal mobile data (3G, 4G, or 5G).
- The school's network incorporates **age-appropriate filtering and active monitoring** systems designed to reduce exposure to harmful or inappropriate content.
- Filtering and monitoring systems are configured to identify and alert the **DSL** and **ICT Technician** to safeguarding risks, including attempts to access restricted material.
- The school takes a **risk-based approach**, applying stricter filters for younger pupils (EYFS/KS1) and more educational autonomy for older pupils (KS2), always within a safeguarded framework.
- Staff and pupils must **not attempt to bypass or disable** school filters, connect to unauthorised networks, or use VPNs or mobile hotspots on site.

## 18.3 Oversight and Review

- The **ICT Technician** and **DSL** review filtering and monitoring logs **half-termly** and report findings to the **Safeguarding Link Governor**.
- An **annual audit** of filtering and monitoring is conducted to ensure compliance with the **DfE Filtering and Monitoring Standards (2024)** and any emerging risks.

- Any alerts relating to potential safeguarding issues are logged on **CPOMS** and investigated by the **DSL** in collaboration with the **Headteacher**.
- The school maintains **written assurances** from its filtering and monitoring providers confirming compliance with DfE standards.

## 18.4 Cyber Security and Privacy

- Network access is secured through **unique logins, strong password protocols, and multi-factor authentication** for staff.
- The **ICT Technician** ensures that all systems, software, and devices are kept up to date with appropriate patches and security measures.
- All internet activity is logged and monitored in accordance with **UK GDPR**, **Data Protection Act (2018)**, and the school's **Data Protection Policy**.

---

# 19. Filtering and Monitoring Online Activity

Gatehouse School recognises that robust filtering and monitoring systems are essential to safeguard pupils from harmful online content and activity, in line with the DfE's *Filtering and Monitoring Standards for Schools and Colleges (2023)*, updated **KCSIE 2025** expectations, and UK Safer Internet Centre guidance.

## 19.1 Roles and Responsibilities

- The **DSL** ensures that filtering and monitoring arrangements are effective, proportionate, and aligned with the school's safeguarding risk assessment; the DSL also escalates significant concerns to the Headteacher or governing body.
- The **ICT Technician** manages day-to-day configuration, maintenance, and testing of systems, documenting all checks, incidents, and changes.
- The **Headteacher** provides strategic oversight, approves major configuration changes following risk assessment, ensures leadership understanding of filtering/monitoring, and supports escalation of issues.
- The **Safeguarding Link Governor** receives termly reports on filtering, monitoring, and any escalations, enabling governance oversight and challenge.
- **All staff** understand their duty to report suspected breaches, safeguarding alerts, or system failures to the DSL immediately.

## 19.2 Risk Assessment and Proportionality

- The Headteacher and ICT Technician conduct a formal risk assessment to determine appropriate filtering/monitoring levels, considering:
    - Pupils' age, development, and vulnerability;
    - Number of users, device types, and usage patterns;
    - Types of online activities (including AI-generated content, misinformation/disinformation, and evolving digital risks);

    - Educational needs and safeguarding impact.

- The DSL ensures that *over-blocking* does not unnecessarily restrict legitimate teaching, research, or access to safeguarding resources.
- The system must address **AI-generated content**, and manage real-time responses from generative tools.
- The system must include **IWF and CTIRU blocklists**, which must not be disabled or removed by administrators or users.

## 19.3 System Maintenance, Checks & Change Control

- The ICT Technician conducts **monthly operational checks** and **annual deep reviews**, including real-world testing (e.g. via test pages or TestFiltering tools) to verify filter efficacy.
- Any requested changes to configurations must be submitted to the Headteacher (or DSL) for review and authorization, following a documented risk assessment.
- Supplier assurances or updates must be obtained at least annually, to demonstrate alignment with DfE/UKSIC standards.

## 19.4 Incident Reporting and Escalation

- Reports of access to inappropriate or harmful content are immediately directed to the ICT Technician, who investigates and remediates.
- All incidents, breaches, or system failures are logged (e.g. in CPOMS or equivalent) and escalated to the DSL for review.
- **Deliberate breaches** of filtering policies are managed via:
    - **Pupils** - under the Behaviour Policy;
    - **Staff** - under the Staff Code of Conduct / disciplinary procedures.
- If material accessed is believed to be **illegal**, the school immediately contacts relevant authorities (e.g. Internet Watch Foundation, CEOP, police) and treats this as a serious safeguarding incident.

## 19.5 Monitoring and Privacy

- The school network and devices are **actively monitored** for safeguarding, policy compliance, and cyber-security risks.
- Users (staff, pupils, parents) are informed via Acceptable Use and consent agreements about how and why monitoring occurs, in compliance with UK GDPR and the Data Protection Act 2018.
- Alerts or flagged risks are reviewed by the DSL and ICT Technician, who decide on internal intervention, safeguarding follow-up, or external referral.
- Monitoring logs must be retained securely and reviewed **at least every half term**, with summaries reported to the DSL.

## 19.6 Continuous Improvement and Review

- The DSL and ICT Technician conduct a **termly review** of filtering/monitoring effectiveness (e.g. reviewing alerts, feedback, test outcomes).
- The school will annually use the DfE's *Plan Technology for Your School* self-assessment tool to benchmark and refine its arrangements.
- Lessons from incidents or near-misses will be shared with staff to improve awareness and practice.
- Findings and key metrics are reported to the Safeguarding Link Governor and included in the annual safeguarding report to the governing board.

---

# 20. Network Security

Gatehouse School is committed to maintaining a secure and resilient ICT network that protects pupils, staff, and school data. Network security underpins our **Champion Values** of *Accountability* and *Integrity* and forms a core part of our safeguarding practice.

## 20.1 Oversight and Responsibility

- The **ICT Technician** manages technical network security and reports to the **Headteacher** and **DSL**.
- The **Headteacher** holds overall responsibility for ensuring compliance with the *DfE Cyber Security Standards for Schools and Colleges (2024)* and *Keeping Children Safe in Education (2025)*.
- The **DSL** oversees the safeguarding aspects of cyber incidents, ensuring any breaches or risks are logged and investigated via **CPOMS**.

## 20.2 Technical Controls

- Up-to-date **anti-virus and anti-malware software** is installed on all devices and automatically updated.
- **Firewalls** are enabled at all times and reviewed **weekly** by the ICT Technician to ensure correct operation and version updates.
- All systems use **multi-factor authentication (MFA)** for staff administrative access and **encryption** for data in transit and at rest.
- **Automatic backups** are performed regularly, stored securely off-site or in the cloud, and tested termly for recovery integrity.
- Devices and network systems are patched and updated promptly according to the school's **Cyber Security Policy**.

## 20.3 Access Control and Passwords

- Each member of staff has a **unique username and private password** to access school systems.
- Pupils (from Key Stage 1 upwards) are issued individual logins with age-appropriate permissions.
- Passwords:
    - Must meet complexity requirements (letters, numbers, symbols, minimum length).
    - Expire every **90 days** and must be changed immediately if compromised.
    - Must never be shared or written down.
- Users are required to **lock their screens or log off** when devices are unattended.
- Forgotten credentials are reset only by the ICT Technician following identity verification.
- Any suspected password sharing or unauthorised access is reported to the **Headteacher** and managed under the **Staff Code of Conduct** or **Behaviour Policy**.

## 20.4 User Conduct and Safe Practice

- Staff and pupils must not download or install **unapproved software** or apps on school devices.
- All users must treat unfamiliar email attachments and links with caution and **report any suspected phishing, malware or ransomware** activity immediately to the ICT Technician.
- Personal devices connecting to the school network must comply with the **Staff and Pupil Acceptable Use Agreements (AUA)**.

## 20.5 Incident Response and Review

- Any cyber-security incident, malware detection, or network breach is reported to the **ICT Technician**, who immediately informs the **DSL** and **Headteacher**.
- Incidents are recorded on **CPOMS** and investigated

- Where required, the school will notify the **ICO** (Information Commissioner's Office) in line with *UK GDPR* breach-reporting requirements.
- Lessons learned from incidents are reviewed termly and shared through staff training and the **Online Safety Action Plan (Appendix 1)**.

## 20.6 Continuous Improvement

- The ICT Technician conducts **quarterly security audits** and reports findings to the Headteacher and **Safeguarding Link Governor**.
- Annual penetration-testing or external audit is commissioned where appropriate.
- Network-security measures are reviewed annually.

# 21. Emails

Access to and the use of school email accounts are managed in accordance with the **Data Protection Policy**, **Cyber Security Policy**, and **Acceptable Use Agreements (AUA)**.

## 21.1 Account Access and Authorisation

- All staff and pupils are provided with **approved Gatehouse School email accounts** for educational and professional use only.
- Personal email accounts **must not be used for school business** under any circumstances.
- Before being granted access, all users must read and sign the appropriate **Acceptable Use Agreement**.
- Email accounts are protected by **secure passwords and multi-factor authentication (MFA)** in line with the *DfE Cyber Security Standards (2024)*.
- Staff must ensure that their school email remains professional in tone and content and is used only for legitimate school purposes.

## 21.2 Data Protection and Encryption

- Any email containing **personal or sensitive data** must be sent using **encryption** (e.g. secure email systems or password-protected attachments).
- Email communication must comply with the **UK GDPR** and **Data Protection Act (2018)** principles.
- The **DPO** (or Headteacher, where appropriate) must be consulted if a data breach occurs or is suspected.

## 21.3 Email Monitoring and Filtering

- The school's email systems are monitored in line with the **Filtering and Monitoring Policy**, and can detect:
    - Inappropriate links or attachments.
    - Profanity or harmful content.
    - Suspicious external addresses.
- All users are informed that their emails may be monitored and recorded for **safeguarding and data-protection purposes**.
- Any safeguarding concerns arising from email correspondence are logged on **CPOMS** and reviewed by the **DSL**.

## 21.4 Spam, Phishing, and Malicious Emails

- Staff and pupils must immediately **block or report** any suspicious, spam, or junk messages to the **ICT Technician**.

- Emails from unknown sources, chain letters, and clickbait messages should be **deleted without opening**.
- The ICT Technician delivers an **annual assembly and staff briefing** on recognising phishing and malicious emails, covering:
    - How to identify legitimate versus suspicious email addresses.
    - Common phishing tactics and urgent “call to action” wording.
    - The importance of checking spelling, grammar, and tone for warning signs.
    - Reporting procedures for suspected phishing attempts.
- Staff participate in **cyber-awareness training** and periodic **phishing simulations** as part of the school’s ongoing cyber-security development plan.

## 21.5 Incident Management

- Any cyber attack or data breach initiated via email will be managed under the **Cyber Incident Response and Recovery Plan**.
- The **ICT Technician** immediately informs the **Headteacher**, **DSL**, and **DPO** of the breach, and appropriate action is taken to contain and investigate the incident.
- Where personal data may have been compromised, the **ICO** is notified in accordance with *UK GDPR* requirements.
- Lessons learned from any incident are recorded and used to update training and procedures.

---

# 22. Generative AI

Gatehouse School recognises that artificial intelligence (AI) and generative technologies present significant opportunities for learning and creativity, while also introducing new safeguarding, ethical, and data-protection considerations.

## 22.1 Curriculum and Education

- The school prepares pupils to understand and use **emerging technologies**, including generative AI, safely and responsibly.
- Learning about AI is tailored to pupils’ age and understanding, focusing on:
    - What AI is and how it works in simple, age-appropriate terms.
    - How generative tools (e.g. chatbots, image creators) can be used positively for creativity and problem solving.
    - The risks of bias, misinformation, and plagiarism associated with AI.
    - The importance of applying **critical thinking** when engaging with AI-generated content.
- Teachers model responsible use of AI in learning contexts and reinforce the principle that AI must support, not replace, independent thought or effort.

## 22.2 Safeguarding and Filtering Controls

- The school's ICT systems include **appropriate filtering and monitoring** to limit pupils' ability to access or generate harmful or inappropriate content through AI tools.
- AI access is restricted on the school network unless it has been **reviewed and approved** by the **ICT Technician** and **DSL**.
  Any use of AI that produces or accesses unsafe or age-inappropriate material is reported to the **DSL** and logged on **CPOMS**.
- Staff and pupils are regularly reminded that all online activity, including AI use, is subject to school monitoring in line with the **Online Safety Policy** and **Acceptable Use Agreements**.

## 22.3 Data Protection and Ethical Use

- No personal, identifiable, or sensitive data will ever be entered into any generative-AI platform by pupils or staff.
- The school ensures compliance with the **UK GDPR** and **Data Protection Act (2018)** when evaluating or using AI tools.
- Staff are reminded that uploading real pupil data, assessment work, or staff information into third-party AI systems could constitute a **data breach**.
- AI tools may only be used with **anonymised or fictional data** for educational purposes.
- Where AI-generated outputs are used, staff and pupils are encouraged to **verify accuracy** and **acknowledge AI involvement** transparently.

## 22.4 Staff Responsibilities and Oversight

- Staff use AI in accordance with the **Staff Acceptable Use Agreement** and only for approved educational or administrative purposes.
- The **DSL** and **ICT Technician** jointly monitor AI-related use, incidents, or concerns, ensuring that risks are managed appropriately.
- The **Headteacher** ensures that AI-related systems, filtering, and training are reviewed annually and that **governors** are informed of emerging trends or updates.
- All incidents or near misses involving AI misuse or data exposure are reported and investigated in line with the **Cyber Incident Response Plan**.

## 22.5 Training and Continuous Improvement

- Staff receive **annual updates and training** on AI use, data protection, and ethical considerations.
- The school will continue to engage with **DfE, UK Safer Internet Centre**, and **National Cyber Security Centre (NCSC)** guidance to maintain a safe, secure, and reliable foundation before adopting more powerful AI tools.
- Governors will be briefed termly on AI developments, ensuring appropriate challenge and strategic oversight.

# 23. Social Networking

The use of social media by staff and pupils will be managed in line with the **Social Media Policy**, **Acceptable Use Agreements (AUA)**, and **Staff Code of Conduct**.

## 23.1 Purpose and Principles

Gatehouse School recognises that social-media platforms can support communication, creativity, and community engagement.

## 23.2 Staff Use

- Staff use only authorised, school-approved accounts for professional communication with pupils, parents, or the public.
- Personal social-media accounts must never be used to contact or follow pupils or parents.
- Staff are expected to maintain the highest standards of professionalism online, ensuring that privacy settings, posts, and affiliations cannot bring the school into disrepute.
- Any online content referring to the school must be accurate, respectful, and approved where required by the **Headteacher** or **Marketing Lead**.
- Breaches are managed in line with the **Staff Code of Conduct** and **Disciplinary Policy**.

## 23.4 Pupil Use

- Pupils are educated through **Computing** and **PSHE/RHE** about responsible and ethical use of social media.
- Pupils must not post, share, or comment in ways that could harm others, reveal personal information, or damage the school's reputation.
- Cyberbullying, harassment, or sharing of indecent images online will be dealt with under the **Behaviour Policy** and **Child Protection and Safeguarding Policy**.
- The school promotes kindness, empathy, and accountability in all online interactions.

## 23.5 Monitoring and Safeguarding

- Any safeguarding concern arising from social-media activity is reported to the **DSL** and logged on **CPOMS**.
- The **DSL** and **ICT Technician** monitor emerging trends and provide regular updates and guidance to staff, pupils, and parents.
- Staff receive annual training on social-media conduct, privacy settings, and recognising online risk indicators.

## 23.6 Official School Accounts

- The school's official social-media accounts are managed centrally and used solely for positive communication, promotion, and celebration of school life.
- Content is approved in line with the **Digital Images and Marketing Policy**, ensuring compliance with **UK GDPR** and parental permissions.
- Passwords and access rights to official accounts are controlled by the **Headteacher** and **Marketing Officer** and **pre-approved staff**.

---

# 24. The School Website

The **Headteacher** holds overall responsibility for the content, accuracy, and security of the Gatehouse School website. They ensure that all published material is appropriate, accurate, and up to date, and that the website meets the requirements of the **Independent School Standards (ISI, 2025)** and **DfE statutory publication regulations**.

## 24.1 Purpose and Principles

The school website is an important communication tool, it promotes transparency, celebrates achievements, and provides essential information for current and prospective parents, pupils, and staff.

## 24.2 Content Management and Oversight

- The **Headteacher** has final approval of all website content.
- The **Marketing Officer** and designated **Website Administrator** manage day-to-day updates, ensuring information is accurate, compliant, and professional in tone.
- Key statutory information is reviewed **at least termly** to ensure compliance, including:
    - Safeguarding and Child Protection Policy
    - Curriculum details by subject and year group
    - Governance and proprietorial information
    - Pupil performance data (where relevant)
    - Admissions arrangements
    - Equality and SEND information
    - Contact details for the school and key staff
- Outdated or inaccurate information must be corrected immediately once identified.

## 24.3 Data Protection and Privacy

- The website complies with the **UK GDPR** and **Data Protection Act (2018)**.
- No personal information about pupils or staff will be published without consent in line with the **Digital Images Policy** and **Privacy Notice**.

- Pupils are identified by **first name only** (or anonymously) in published content or photographs.
- All photographs and videos must be approved by the **Headteacher** or delegated lead and cross-checked against the parental permission list maintained by the school office.
- The school website will not include any material likely to compromise the safety or privacy of pupils, staff, or families.

### 24.4 Monitoring and Review

- The **Headteacher** conducts an **annual website compliance audit** against ISI and DfE publication standards to ensure that all statutory information, policies, and documentation published online are accurate, current, and accessible to parents, pupils, and stakeholders.
- Any breaches, errors, or inappropriate content are reported to the **DSL** and **ICT Technician**, logged on **CPOMS** if relevant, and rectified immediately.

---

## 25. Use of Devices

Staff members and pupils may be issued with **school-owned devices** to support teaching, learning, and administrative duties, where necessary.

The allocation, use, and management of these devices are governed by the school's **Asset Management and ICT Security Policies**, which outline expectations for responsible use, storage, and return.

Users must:

- Use devices **only for authorised educational or professional purposes**.
- Follow the school's **Acceptable Use Agreements** and **Cyber-Security Policy**.
- Ensure devices remain password-protected and data is stored securely.
- Report any **loss, damage, or security incident** (e.g. unauthorised access, data breach) immediately to the **ICT Technician** and **DSL**.

All school-owned devices are subject to the school's **monitoring and filtering systems**. Any misuse of school-owned devices will be addressed under the **Behaviour Policy** (for pupils) or **Staff Code of Conduct / Disciplinary Policy** (for staff).

---

## 26. Remote Learning

All remote or hybrid learning will be delivered in accordance with the school's **Remote Education Policy**, which outlines safeguarding and online safety measures in full.

The school ensures that:

- Online learning takes place only via **approved platforms** that meet **DfE and UK GDPR standards** for data security and privacy.
- Staff and pupils follow the relevant **Acceptable Use Agreements** and the **Staff Code of Conduct** when engaging in remote education.
- The same high expectations for behaviour, conduct, and communication apply during online lessons as in face-to-face teaching.
- Parents and carers are informed of the arrangements for remote learning and encouraged to supervise pupil engagement where appropriate.
- Any concerns about online safety or pupil wellbeing during remote learning are reported immediately via **CPOMS** to the **DSL**, who will respond in line with the **Child Protection and Safeguarding Policy**.

Remote education is designed to maintain a safe, structured and inclusive digital learning environment that upholds the **Gatehouse Champion Values** and promotes pupils' responsible and respectful use of technology.

---

# 27. Links to other Policies, Legislation and Guidance Documents

## 27.1 Relevant Internal Documents

This policy should be read in conjunction with the following policies and documents.

- Prevent Duty Policy
- Social Media Policy
- 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
- Health and Safety Policy
- Remote Education Policy

- Home School Agreement
- SEND Policy
- Social, Emotional and Mental Health Policy
- WhatsApp Policy (Parents)

## 27.2 Relevant External Documents

Relevant external documents to refer to are the:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) ‘Filtering and monitoring standards for schools and colleges’
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2025) ‘Keeping children safe in education 2025’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2022) ‘Searching, screening and confiscation’
- DfE (2023) ‘Generative artificial intelligence in education’
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’
- Independent School Standards Regulations (DfE, 2014, as amended)
- The Prevent Duty (Counter-Terrorism and Security Act 2015)

---

# Appendix 1 - Online Safety Action Plan

**Purpose:**
To ensure that Gatehouse School maintains robust, effective, and proportionate online safety systems in line with *Keeping Children Safe in Education (2025)*, the *DfE Filtering and Monitoring Standards (2024)*, and the *UK Safer Internet Centre's Appropriate Filtering and Monitoring Definitions (2025)*.

| Priority Area | Actions / Tasks | Lead / Responsibility | Timescale / Review | Evidence / Monitoring | Status |
|---|---|---|---|---|---|
| **1. Filtering and Monitoring Compliance** | Review filtering configuration against DfE (2024) and UKSIC (2025) standards. Verify inclusion of IWF and CTIRU blocklists and AI-content filters. | ICT Technician / DSL | Termly review | Technical audit logs; supplier assurances; test-page checks | |
| **2. Risk Assessment and Oversight** | Update filtering and monitoring risk assessment, including AI-generated content, misinformation/disinformation, and age-appropriate proportionality. | DSL / Headteacher | Termly | Signed risk assessment; minutes from DSL review | |
| **3. Staff Understanding and Training** | Deliver CPD on online safety, data protection, and recognising new online harms (AI, fake news, deepfakes). Include induction training. | DSL / Headteacher / ICT Lead | Autumn 2025; refreshed annually | Training log; staff sign-off; evaluation forms | |
| **4. Pupil Digital Literacy** | Embed online safety and media-literacy lessons (fake news, AI ethics, cyberbullying, privacy) within Computing and PSHE. | Computing Lead / Class Teachers | Ongoing; reviewed termly | Lesson plans; pupil voice; curriculum maps | |

| | | | | | |
|---|---|---|---|---|---|
| **5. Parental Engagement** | Provide termly communication (newsletter, workshop, or Google Classroom post) explaining how filtering and monitoring protect pupils and how parents can support online safety at home. | DSL / Marketing Team | Termly | Copies of newsletters; attendance records; feedback forms | |
| **6. System Testing and Review** | Conduct monthly technical checks and an annual deep review of filtering effectiveness, including live test-page scenarios. Record actions taken. | ICT Technician | Monthly / Annually | Audit checklist; change-log report | |
| **7. Incident Management** | Ensure all online safety concerns are logged on CPOMS and reviewed by DSL within 24 hours. Evaluate outcomes to identify trends and improvements. | All Staff / DSL | Ongoing | CPOMS data report; safeguarding meeting minutes | |
| **8. Data Protection & Privacy** | Confirm monitoring systems comply with UK GDPR; review Acceptable Use Agreements to ensure users are informed about monitoring. | DPC / DSL | Annual review | Updated AUA; privacy notice | |
| **9. Governance Oversight** | Provide termly summary of filtering/monitoring logs, incidents, and actions to the Safeguarding Link Governor. | DSL / Headteacher | Termly | Governor minutes; safeguarding report | |
| **10. Continuous Improvement** | Use DfE's *Plan Technology for Your School* self-assessment tool annually to benchmark provision and inform next steps. | DSL / ICT Technician | Annual ( Summer Term ) | Completed self-assessment and updated action plan | |