



# Online Safety and Social Media Policy

Lead staff member: **Mr L. Hale, Head of School**

Policy adopted by the governing body in **September 2026**

To be reviewed in **September 2027**

# Contents

1. Purpose and scope
  2. Aims
  3. Legal and guidance framework
  4. Understanding online risk
  5. Roles and responsibilities
  6. Filtering and monitoring
  7. Teaching online safety
  8. Supporting pupils who may be more vulnerable
  9. Acceptable use of technology
  10. Mobile phones, smart watches and personal devices
  11. Staff use of technology and school devices
  12. Social media and professional boundaries
  13. Images, photographs, video and livestreaming
  14. Online learning, communication and cloud services
  15. Artificial intelligence
  16. Responding to online safety incidents
  17. Online bullying and child-on-child abuse
  18. Training and awareness
  19. Working with parents and carers
  20. Monitoring, evaluation and review
- Appendix 1: Incident response guide
- Appendix 2: Links with other school policies

# 1. Purpose and scope

This policy sets out how Deighton Gates Primary School promotes safe, responsible and respectful use of technology and responds to online safety concerns. It forms part of the school's wider safeguarding arrangements and should be read alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy and Acceptable Use Agreements.

The policy applies whenever school technology, accounts, networks, platforms or data are used. It also applies to online activity outside school where that activity creates a safeguarding concern, affects pupils' welfare, disrupts school life, damages professional boundaries or brings the school into disrepute.

The policy covers internet access, email, cloud services, social media, online learning platforms, mobile phones, smart watches, cameras, messaging, gaming, livestreaming, artificial intelligence and any other connected or digital technology.

## 2. Aims

Deighton Gates Primary School aims to:

- Protect pupils, staff and the wider school community from online harm.
- Ensure that online safety is understood as an integral part of safeguarding, not solely as a computing or technical issue.
- Provide clear systems for identifying, reporting, recording, responding to and escalating concerns.
- Maintain filtering and monitoring arrangements that reflect the school's safeguarding needs while enabling effective teaching and learning.
- Teach pupils the knowledge, skills and habits needed to use technology safely, critically, respectfully and responsibly.
- Help pupils recognise unreliable information, manipulation, harmful contact, persuasive design and commercial risks.
- Support parents and carers to understand current online risks and reinforce safe practice at home.
- Set clear expectations for staff conduct, professional boundaries, confidentiality and the use of social media.
- Adapt teaching, supervision and support for pupils whose needs or circumstances increase their vulnerability online.

## 3. Legal and guidance framework

This policy has regard to current statutory and non-statutory guidance, including:

- Department for Education, Keeping Children Safe in Education.
- Department for Education, filtering and monitoring standards for schools and colleges.
- Department for Education, Teaching online safety in schools.
- Department for Education, Searching, screening and confiscation at school.
- Department for Education, Preventing and tackling bullying and advice on cyberbullying.
- Department for Education, Relationships Education, Relationships and Sex Education and Health Education guidance.
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes and other relevant online harms.
- The Education Act 1996, Education and Inspections Act 2006, Education Act 2011, Equality Act 2010, Data Protection Act 2018 and UK General Data Protection Regulation.
- The Prevent duty and current guidance on protecting children from radicalisation.
- The National Curriculum programmes of study for computing.

Where guidance is updated during the lifetime of this policy, the school will follow the current version and amend local procedures where necessary.

## 4. Understanding online risk

The school's approach addresses four connected areas of risk:

| Area            | Examples                                                                                                                                                                                                                 |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Content</b>  | Exposure to illegal, inappropriate or harmful material, including violent or sexual content, self-harm or suicide content, hate, extremism, misinformation, disinformation, deepfakes and harmful AI-generated material. |
| <b>Contact</b>  | Harmful interaction with others, including bullying, coercion, grooming, exploitation, impersonation, pressure from peers, contact from unknown adults and persuasive commercial contact.                                |
| <b>Conduct</b>  | A person's own online behaviour, including unkind or abusive communication, oversharing, unsafe livestreaming, sharing intimate images, creating or distributing harmful content and breaching privacy or copyright.     |
| <b>Commerce</b> | Online gambling, scams, phishing, in-game purchasing, inappropriate advertising, financial exploitation and pressure to spend money.                                                                                     |

## 5. Roles and responsibilities

### 5.1 Governing Body

The Governing Body provides strategic oversight and holds leaders to account for the effectiveness of this policy. It will:

- Ensure that online safety is embedded within the school's safeguarding arrangements.
- Ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually.
- Ensure that responsibilities for filtering and monitoring are clearly assigned.
- Receive appropriate information about online safety risks, incidents, training and the effectiveness of controls.
- Ensure that staff receive suitable safeguarding and online safety training and updates.
- Approve this policy and review assurance from leaders.

### 5.2 Executive Headteacher

The Executive Headteacher retains overall accountability for safeguarding and will ensure that the school has appropriate leadership, staffing, resources, systems and technical support to implement this policy.

### 5.3 Head of School

The Head of School is responsible for the day-to-day implementation of this policy at Deighton Gates. The Head of School will:

- Act as the Designated Safeguarding Lead (see additional responsibilities below)
- Ensure that staff understand and consistently apply the policy.
- Ensure that online safety is reflected in curriculum, behaviour, safeguarding and staff conduct arrangements.
- Ensure that actions arising from incidents, reviews or audits are completed.
- Work with the Computing Lead and IT support provider to resolve operational concerns.
- Report significant concerns and assurance information to the Headteacher and Governing Body.

### 5.4 Designated Safeguarding Lead

The DSL has lead responsibility for online safety as a safeguarding matter. The DSL will:

- Understand the filtering and monitoring systems and processes used by the school.
- Define the school's safeguarding needs for filtering and monitoring, with support from leaders and technical staff.
- Receive, assess and coordinate responses to online safeguarding concerns.
- Ensure that concerns and decisions are recorded in accordance with safeguarding procedures.
- Liaise with children's social care, the police, the local authority or other agencies where required.

- Ensure that staff know how to report concerns, alerts and suspected weaknesses in controls.
- Contribute to staff training, pupil education, parental awareness and policy review.
- Provide leaders and governors with appropriate information about themes, risks and effectiveness without compromising confidentiality.

## 5.5 Computing Lead

The Computing Lead will oversee progression in online safety education through the computing curriculum, support staff with curriculum resources, evaluate implementation and work with the DSL so that teaching reflects current safeguarding risks.

## 5.6 IT support provider

The school's contracted IT support provider will implement and maintain approved technical controls. In partnership with school leaders, it will:

- Maintain filtering, monitoring, security, device management, updates and access controls.
- Provide reports or access to information needed for safeguarding review.
- Escalate significant technical weaknesses, attempted bypasses and relevant alerts promptly.
- Support annual and event-driven reviews of filtering and monitoring.
- Implement approved changes without unreasonably restricting teaching and learning.
- Support secure account management, authentication, backup and incident recovery.

## 5.7 All staff, volunteers and contractors

- Read, understand and follow this policy, the Staff Code of Conduct and relevant Acceptable Use Agreement.
- Maintain professional curiosity and an attitude that online harm could happen here.
- Report safeguarding concerns immediately through the school's safeguarding procedures.
- Report filtering or monitoring weaknesses, inappropriate access and suspected security incidents promptly.
- Use only approved systems, accounts and communication channels for school business.
- Supervise pupils' use of technology appropriately and reinforce safe expectations.
- Do not investigate safeguarding concerns beyond what is necessary to establish immediate facts and protect the child.
- Preserve evidence only in line with DSL, police or specialist advice and do not unnecessarily view, copy, print, forward or store illegal or indecent material.

## 5.8 Pupils

Pupils will be taught and expected to use technology safely, respectfully and responsibly; protect personal information and passwords; follow staff instructions and Acceptable Use Agreements; and tell a trusted adult if something online causes concern, worry or harm.

## 5.9 Parents and carers

Parents and carers are expected to support the school's online safety expectations, discuss safe technology use with their child, alert the school to relevant concerns and avoid online activity that compromises the privacy, safety or dignity of pupils, families or staff.

# 6. Filtering and monitoring

**Core expectation** Filtering and monitoring will be proportionate to the school's safeguarding needs, effective across school-owned devices and networks, reviewed at least annually and managed without unreasonably limiting teaching and learning.

The school will:

- Identify and assign roles for strategic oversight, safeguarding decisions, technical management, alert review and escalation.

- Use filtering to block harmful and inappropriate content, including illegal content, while maintaining suitable access for education and school business.
- Use monitoring strategies capable of identifying concerning activity and supporting a timely safeguarding response.
- Ensure that staff know what is monitored, who receives alerts and how to report concerns or weaknesses.
- Apply appropriate controls to different users, age groups, devices and contexts.
- Take reasonable steps to prevent users from bypassing controls, including through proxy services, personal hotspots or unauthorised software.
- Record decisions to allow, restrict or unblock material where the decision is significant or safeguarding-related.
- Consider the implications of encrypted traffic, cloud applications, personal devices and new technologies.

## 6.1 Review arrangements

The Head of School (inc. DSL), Computing Lead and IT support provider will complete a documented review at least annually. The review will also be revisited following a serious incident, significant system change, identified weakness or material change in risk.

The review will consider:

- Whether roles and escalation routes remain clear.
- Whether filtering categories and exceptions reflect pupils' ages, curriculum needs and local safeguarding risks.
- Whether monitoring produces usable information and whether alerts are reviewed promptly.
- Whether school-owned devices are protected when used away from the school network.
- Whether logs, reports, testing and staff feedback indicate gaps or over-blocking.
- Whether actions from the previous review have been completed.

## 6.2 Requests to change access

Staff must use the agreed request process when a legitimate educational or operational resource is blocked. Staff must not use workarounds or personal accounts to bypass controls. Requests involving safeguarding risk will be referred to the DSL; technical changes will be implemented only by authorised personnel.

# 7. Teaching online safety

Online safety will be taught explicitly and revisited throughout the curriculum. It will not be confined to a single annual lesson or event. Teaching will draw on computing, Relationships and Health Education or PSHE, safeguarding education, assemblies, class discussion and responsive teaching following emerging issues.

Pupils will be taught, at an age-appropriate level, to:

- Use technology safely, respectfully and responsibly.
- Recognise reliable and unreliable information, including manipulated images, misinformation, advertising and AI-generated content.
- Understand that people may behave differently online or misrepresent who they are.
- Protect personal information, privacy, accounts and passwords.
- Recognise harmful content, unsafe contact, pressure, bullying, scams and attempts to manipulate or exploit.
- Understand consent, boundaries and respectful communication in digital contexts.
- Manage screen use, persuasive design, notifications and commercial pressure.
- Seek help, block or report users and content, preserve appropriate evidence and tell a trusted adult.
- Understand that online actions can have lasting consequences for themselves and others.
- Respect copyright, ownership and attribution when using or creating digital material.

Safer Internet Day and other campaigns may be used to reinforce learning, but they do not replace planned, progressive curriculum provision.

## 8. Supporting pupils who may be more vulnerable

The school recognises that vulnerability online is not the same for every child. Age, SEND, communication needs, social isolation, prior trauma, care experience, family circumstances, mental health needs or previous victimisation may affect risk and a pupil's ability to recognise, resist or report harm.

The school will adapt teaching, language, resources, supervision and reporting routes; provide repetition or personalised support where needed; and involve parents, carers and external professionals when appropriate. Safeguarding responses will consider the child's communication profile and avoid assumptions that a child's behaviour indicates informed consent or understanding.

## 9. Acceptable use of technology

All users must follow the Acceptable Use Agreement relevant to their role. School technology and internet access are provided for authorised educational, safeguarding, administrative and professional purposes.

Users must not:

- Access, create, store or share illegal, harmful, abusive, discriminatory or otherwise inappropriate material.
- Attempt to bypass filtering, monitoring, authentication, device management or other security controls.
- Share passwords, use another person's account or leave an active account available to others.
- Install software, browser extensions or applications without authorisation.
- Use unauthorised cloud storage, personal email or consumer messaging services for school information.
- Deliberately damage equipment, interfere with networks or compromise another user's work.
- Use technology to bully, threaten, impersonate, harass, exploit or embarrass another person.
- Disclose personal, confidential or safeguarding information without an appropriate lawful purpose.

Internet and system activity may be filtered, logged and monitored in accordance with safeguarding, security, data protection and employment requirements. Users should not expect personal privacy when using school systems, while recognising that monitoring will be lawful, proportionate and appropriately controlled.

## 10. Mobile phones, smart watches and personal devices

Pupils must not use personal mobile phones, smart watches or other connected devices during the school day unless a specific adjustment or educational use has been approved by the Head of School. The school's current operational arrangements will set out whether devices may be brought to school, how they must be stored and how they are returned.

Where a pupil has an authorised device in school:

- The device must be switched off or placed in the agreed mode and stored as directed.
- The pupil must not take photographs, record audio or video, make calls, send messages or access online services without permission.
- The school is not responsible for loss or damage except where legal responsibility applies.
- Misuse will be addressed under the Behaviour Policy and may also require a safeguarding response.

Staff personal devices must be used in line with the Staff Code of Conduct. Personal phones must not be used to photograph pupils, record safeguarding evidence, communicate privately with pupils or store school information unless an exceptional, authorised process explicitly permits it.

## 11. Staff use of technology and school devices

Staff must take reasonable steps to protect school devices, accounts and information. Staff will:

- Use strong, unique passwords and multi-factor authentication where required by the school.
- Lock devices, including laptops, when unattended and prevent access by family members or other unauthorised people.
- Install updates and security controls as directed and not disable device management or protective software.
- Use approved storage and communication systems and avoid downloading sensitive information where it is not necessary.

- Report lost or stolen devices, suspected account compromise, phishing and data breaches immediately.
- Position screens and conduct calls or online meetings so that confidential information cannot be seen or overheard.
- Return equipment and school information when requested or when employment ends.

School devices must be used in accordance with the Staff Code of Conduct and the school's Acceptable Use Agreement.

## 12. Social media and professional boundaries

The same expectations of professionalism, confidentiality, respect and safeguarding apply online as they do offline. Privacy settings do not remove professional responsibilities, and content intended for a limited audience may be copied or redistributed.

Staff must:

- Use official school channels for communication with pupils and school business.
- Never communicate privately with pupils through personal social media, gaming, messaging or email accounts.
- Not accept or initiate social media connections with current pupils through personal accounts.
- Exercise professional judgement about connections with parents and carers and avoid arrangements that compromise boundaries or create unequal access.
- Never post confidential information about pupils, families, colleagues or school matters.
- Not post images, video or identifying information about pupils except through authorised school processes.
- Not make discriminatory, abusive, defamatory or otherwise unprofessional comments connected to the school community.
- Report safeguarding concerns, impersonation, threats, harassment or boundary breaches using the appropriate school procedure.
- Report concerns about another adult's online conduct promptly in accordance with the school's procedures for low-level concerns, allegations against adults or whistleblowing. Staff should not investigate the concern themselves.

The school may choose to maintain official social media accounts. Where this is the case, only authorised staff may publish through them. Account access, moderation, records, image permissions and responses to direct messages will be managed under agreed school procedures.

## 13. Images, photographs, video and livestreaming

The school will use images and recordings only for an identified educational, administrative or communication purpose and in accordance with data protection, safeguarding and consent or privacy arrangements.

- School images and recordings must be made using authorised equipment or systems.
- Images must be stored securely, retained only as necessary and shared only through approved channels.
- Staff must consider names, uniforms, location data, background detail and other information that could identify or place a child at risk.
- Livestreaming or video calls involving pupils must use approved platforms, suitable access controls and appropriate adult supervision.
- Where photography or recording by families is permitted at an event, the school will remind attendees to act responsibly and not share material in a way that compromises another child's privacy or safety.
- The school may restrict photography or recording where safeguarding, privacy, copyright or the orderly running of an event requires it.

## 14. Online learning, communication and cloud services

Only platforms and cloud services approved by the school may be used for teaching, pupil communication, safeguarding records or school business. The school will consider age restrictions, privacy, security, accessibility, data processing, moderation and safeguarding controls before approving a service.

Staff will use school-managed accounts, apply appropriate access controls, supervise pupil activity and ensure that communication remains visible, professional and auditable. Pupils will be taught not to share login details or invite unauthorised users into school spaces.

## 15. Artificial intelligence

Generative and other forms of artificial intelligence can support teaching and administration, but can also create risks involving inaccurate information, bias, privacy, copyright, impersonation, deepfakes, harmful content and reduced transparency. AI use must therefore be purposeful, age-appropriate, supervised and consistent with school policy.

Staff must:

- Use only AI tools approved for the intended purpose and follow any school guidance or licensing conditions.
- Never enter safeguarding records, special category data, confidential pupil information or identifiable personal data into an unapproved AI service.
- Check AI-generated material for accuracy, bias, suitability, copyright concerns and safeguarding risk before use.
- Remain professionally accountable for decisions, communications, plans and resources, even where AI has assisted.
- Be transparent about AI use where this is relevant to trust, assessment or decision-making.
- Report harmful AI-generated content, impersonation, deepfakes or safeguarding concerns to the DSL.

Pupils may use AI only through arrangements approved and supervised by the school. Teaching will help pupils understand that AI outputs can be convincing but false, biased or unsafe, and that personal information should not be entered into public systems.

## 16. Responding to online safety incidents

Online incidents will be managed according to their nature and seriousness. Some incidents may require a safeguarding response, behaviour response, technical response, data breach response, staff conduct process or criminal referral. More than one process may apply.

When a concern is identified, staff must:

- Protect the child or other person from immediate harm.
- Listen calmly, avoid blame and take the concern seriously.
- Avoid promising confidentiality.
- Establish only the limited facts needed for immediate safety and reporting.
- Report the concern promptly to the DSL or a deputy through the school's safeguarding process.
- Avoid viewing, forwarding, copying, printing or saving illegal or indecent content unless specifically directed by an authorised safeguarding or law-enforcement professional.
- Preserve contextual information such as usernames, URLs, dates and times where safe and appropriate, but do not conduct an independent investigation.
- Follow instructions relating to parents, carers, devices, evidence, external agencies and ongoing support.
- Where an online safety incident raises a safeguarding concern, the Child Protection and Safeguarding Policy and the school's safeguarding reporting procedures take precedence.

The DSL will assess risk, decide immediate protective action, consider the wishes and needs of the child, make referrals where required, oversee recording and coordinate communication. Decisions about informing parents or carers will be made in the child's best interests and will take account of whether doing so could increase risk or compromise an investigation.

## 17. Online bullying and child-on-child abuse

Online bullying and child-on-child abuse may occur on school systems or away from school and may continue beyond the school day. It can include repeated bullying, harassment, threats, hate, coercion, sexualised behaviour, non-consensual image sharing, exclusion, impersonation and abuse within group chats or gaming spaces.

The school will respond even where behaviour began outside school if it affects a pupil's safety, welfare, education or school community. Responses will be proportionate, safeguard all children involved and account for power imbalance, repetition, intent, impact, vulnerability and the possibility that a child who has caused harm may also need protection or support.

Online behaviour will be addressed through the Child Protection and Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy as appropriate. Restorative work will be used only where safe, suitable and consistent with the wishes and welfare of those affected.

## 18. Training and awareness

All staff will receive online safety information during induction and safeguarding training, with updates provided throughout the year. Training will include:

- The role of technology in abuse, exploitation, bullying and wellbeing concerns.
- Current filtering and monitoring arrangements and the responsibilities of staff.
- How to recognise and report online safeguarding concerns and technical weaknesses.
- Professional boundaries, social media, data protection and secure use of devices.
- Emerging risks, including artificial intelligence, manipulated content, scams and new platforms.
- The principle that staff should not investigate or unnecessarily view harmful or illegal material.

The DSL and deputies will maintain current safeguarding knowledge. Governors will receive sufficient training to provide challenge and assurance. Staff with specific curriculum, technical or leadership responsibilities will receive role-appropriate development.

## 19. Working with parents and carers

The school will promote a constructive partnership with parents and carers through newsletters, the school website, workshops, guidance and responsive communication. Information may cover age restrictions, privacy settings, gaming, group chats, devices, parental controls, scams, AI, reporting routes and sources of specialist support.

Parents and carers should raise concerns with the school rather than using social media to identify, criticise or speculate about children, families or staff. Where an online issue affects safeguarding or school life, parents should preserve relevant context and contact the school promptly without redistributing harmful material.

## 20. Monitoring, evaluation and review

The Head of School and DSL will monitor implementation through safeguarding records, filtering and monitoring reviews, curriculum monitoring, pupil voice, staff feedback, incident themes, training records and relevant technical reports.

This policy will be reviewed annually and sooner where there is a significant safeguarding incident, material change to statutory guidance, newly identified risk, substantial technology change or evidence that procedures are not effective. The Governing Body will approve the policy and receive appropriate assurance about implementation.

## Appendix 1: Incident response guide

| Stage             | Required action                                                                                          | Lead             |
|-------------------|----------------------------------------------------------------------------------------------------------|------------------|
| <b>1. Protect</b> | Address immediate safety, stop access or contact where possible, and reassure the pupil.                 | Any staff member |
| <b>2. Report</b>  | Report promptly through safeguarding procedures. Contact the DSL or deputy directly for urgent concerns. | Any staff member |
| <b>3. Assess</b>  | Consider harm, vulnerability, illegality, evidence, parental contact and need for referral.              | DSL or deputy    |

| Stage             | Required action                                                                                     | Lead                              |
|-------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------|
| <b>4. Respond</b> | Coordinate safeguarding, behaviour, technical, data protection or staff conduct action as required. | Relevant lead, coordinated by DSL |

|                  |                                                                                                     |                        |
|------------------|-----------------------------------------------------------------------------------------------------|------------------------|
| <b>5. Review</b> | Record decisions, support those affected, identify lessons and test whether controls need changing. | DSL and Head of School |
|------------------|-----------------------------------------------------------------------------------------------------|------------------------|

**Immediate danger** Call 999 where someone is at immediate risk of serious harm. Staff must still inform the DSL as soon as it is safe to do so.

## Do not

- Promise confidentiality.
- Ask leading or repeated questions.
- Search a pupil's personal device unless authorised under the school's searching arrangements.
- Forward harmful content to another account or device.
- Take screenshots of illegal or indecent images unless specifically directed by police or specialist safeguarding advice.
- Contact an alleged perpetrator or their family before the DSL has assessed risk.
- Post or discuss the incident on social media or informal messaging groups.

## Appendix 2: Links with other school policies

This policy should be read alongside the current versions of:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Low-Level Concerns and Whistleblowing procedures
- Data Protection Policy and Privacy Notices
- Acceptable Use Agreements
- Mobile Phone or Personal Device procedures
- Searching, Screening and Confiscation arrangements
- Curriculum policies for Computing and PSHE or Relationships and Health Education
- Educational Visits Policy
- Complaints Policy
- Records Management and Information Security procedures

## Reference documents

**Keeping Children Safe in Education:** <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

**Filtering and monitoring standards for schools and colleges:** <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

**Teaching online safety in schools:** <https://www.gov.uk/government/publications/teaching-online-safety-in-schools>

**Searching, screening and confiscation at school:** <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

**UK Safer Internet Centre:** <https://saferinternet.org.uk/>

**Childnet:** <https://www.childnet.com/>