

# Online Safety Policy



## Equalities Statement

In our Trust we work to ensure that there is equality of opportunity for all members of our community who hold a range of protected characteristics as defined by the Equality Act 2010, as well as having regard to other factors which have the potential to cause inequality, such as socio-economic factors. For further information, please see our Equalities Policy.

| Document Management |                               |
|---------------------|-------------------------------|
| Version Number:     | 1.0                           |
| Date Approved:      | September 2026                |
| Next Review Date:   | September 2027                |
| Approved By:        | Safeguarding Leadership Group |
| Responsible For:    | Safeguarding Leadership Group |

| Policy Revision Log |                                    |
|---------------------|------------------------------------|
| Date                | Version No. Brief Detail of Change |
|                     |                                    |
|                     |                                    |

## Contents

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| <b>1. Policy Aims</b>                                                       | 4  |
| <b>2. Policy Scope</b>                                                      | 4  |
| 2.1 Links with Other Policies and Practices                                 |    |
| <b>3. Monitoring and Review</b>                                             | 5  |
| <b>4. Roles and Responsibilities</b>                                        | 5  |
| 4.1 The School's Leadership Team and Swale Academy Trust                    |    |
| 4.2 The Designated Safeguarding Lead (DSL)                                  |    |
| 4.3 Members of Staff                                                        |    |
| 4.4 Technical Staff and IT Support (Swale Academies Trust) will             |    |
| 4.5 Learners (commensurate with age and ability) will                       |    |
| 4.6 Parents and Carers                                                      |    |
| <b>5. Education and Engagement Approaches</b>                               | 8  |
| 5.1 Education and Engagement with Learners                                  |    |
| 5.2 Vulnerable Learners & Special Educational Needs and Disabilities (SEND) |    |
| 5.3 Training and Engagement with Staff                                      |    |
| 5.4 Awareness and Engagements with Parents and Carers                       |    |
| <b>6. Responding to Online Safety Incidents and Concerns</b>                | 9  |
| 6.1 Concerns about Learners' Welfare                                        |    |
| 6.2 Staff Misuse                                                            |    |
| <b>7. Procedures for Responding to Specific Incidents or Concern</b>        | 10 |
| 7.1 Child-on-Child Sexual Violence and Sexual Harassment                    |    |
| 7.2 Self-generated Intimate Images and/or Videos                            |    |
| 7.3 Online Child Sexual Abuse and Exploitation                              |    |
| 7.4 Indecent Images of Children                                             |    |
| 7.5 Cyberbullying                                                           |    |
| 7.6 Cybercrime                                                              |    |
| 7.7 Online Hate                                                             |    |
| 7.8 Online Radicalisation and Extremism                                     |    |
| <b>8. Safer Use of Technology</b>                                           | 12 |
| 8.1 Classroom Use                                                           |    |
| 8.2 Managing Internet Access                                                |    |
| 8.3 Filtering and Monitoring (Annual Record Keeping)                        |    |
| 8.4 Managing Personal Data Online                                           |    |
| 8.5 Password Policy and Multi-Factor Authentication                         |    |
| 8.6 Managing the Safety of the Website                                      |    |
| 8.7 Publishing Images and Video Online                                      |    |
| 8.8 Managing Email                                                          |    |
| 8.9 Live Stream Lessons for Remote Learning                                 |    |
| 8.10 Management of Learning Platforms                                       |    |

|                                                          |           |
|----------------------------------------------------------|-----------|
| 8.11 management of Applications (insight)                |           |
| 8.12 Generative Artificial Intelligence                  |           |
| <b>9. Social Media</b>                                   | <b>14</b> |
| 9.1 Expectations                                         |           |
| 9.2 Staff Personal Use of Social Media                   |           |
| 9.3 Learners' Personal Use of Social Media               |           |
| 9.4 Official Use of Social Media                         |           |
| <b>10. Use of Personal Devices and Mobile Phones</b>     | <b>15</b> |
| 10.1 Expectations                                        |           |
| 10.2 Staff Use of Personal Devices and Mobile Phones     |           |
| 10.3 Learners' Use of Personal Devices and Mobile Phones |           |
| 10.4 Visitors' Use of Personal Devices and Mobile Phones |           |
| 10.5 Officially Provided Mobile Phones and Devices       |           |
| <b>11. Useful Links for Education Settings</b>           | <b>16</b> |

## 1. Policy Aims

- This Online Safety Policy has been thoroughly revised and adapted in collaboration with staff, learners, and parents/carers. It builds upon the East Sussex County Council / The Education People online safety policy template, incorporating Swale Academies Trust operational regulations and specialist advice.
- This policy takes direct account of and complies with the DfE Statutory Guidance: Keeping Children Safe in Education (KCSIE) 2026, the Early Years Foundation Stage (EYFS) statutory framework (Section 3), the Data Protection Act 2018, the UK GDPR, and the Data (Use and Access) Act 2025.

### The purpose of this policy is to:

- Safeguard and protect all members of our school community online.
- Identify comprehensive approaches to educate and raise awareness of online safety across the community.
- Enable all staff to work safely, responsibly, and professionally, role-modelling positive behaviours online and maintaining strict professional boundaries.
- Establish clear, legally compliant procedures for responding to online safety incidents.

In line with KCSIE 2026, we recognise that online safety risks are considerable, dynamic, and ever-evolving, and are classified into four areas of risk (the 4 Cs):

- **Content:** Exposure to illegal, inappropriate, or harmful material (e.g., pornography, racism, misogyny, self-harm, suicide, radicalisation, extremism, extreme violence, misinformation, disinformation, "fake news", and conspiracy theories).
- **Contact:** Subjecting learners to harmful online interaction with other users or generative AI applications that simulate such interactions (e.g., peer-to-peer pressure, digital coercive control, commercial exploitation, or adults posing as children/young adults with the intention to groom, abuse, or exploit).
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm (e.g., creating, sending, or receiving explicit images, cyberbullying, or sharing harmful content without consent).
- **Commerce:** Exposure to financial risks (e.g., online gambling, inappropriate advertising, phishing, and/or financial scams).

## 2. Policy Scope

- Online safety is a core component of our statutory safeguarding duties. The school is committed to ensuring all learners and staff are protected from online harms on-site, off-site, and online.
- This policy applies to all staff, including the governing body, trustees, teachers, support staff, supply staff, trainee teachers, external contractors, visitors, volunteers, and other individuals who work for or provide services on behalf of the school (collectively referred to as "staff"). It also applies to all learners, parents, and carers.
- This policy covers all access to the internet and use of digital technologies, whether using personal devices on the school premises or using school-issued devices off-site (such as work laptops, tablets, or mobile phones).
- Under the Education and Inspections Act 2006, the Headteacher has the authority to regulate the behaviour of pupils when they are off the school site. This includes online bullying, harassment, and

online safety incidents that occur outside school hours but impact members of our school family or are linked to the school. The school will actively investigate and address such out-of-school incidents in accordance with this policy, the Behaviour Policy, and the Anti-Bullying Policy, and will notify parents/carers of any findings.

## **2.1 Links with Other Policies and Practices**

This policy must be read and implemented alongside the following statutory and school-specific policies:

- Swale Academies Trust Child Protection and Safeguarding Policy 2026–2027
- Swale Academies Trust Acceptable Use Agreement (AUP)
- Anti-Bullying Policy
- Staff Behaviour Policy / Code of Conduct (including Low-Level Concerns and Whistleblowing)
- Behaviour Policy
- GDPR & Data Protection Policy (updated to reflect the Data (Use and Access) Act 2025)
- School Attendance Policy

*All above policies are available from the school website or from the front office on request.*

## **3. Monitoring and Review**

- Because digital technologies and associated online risks evolve rapidly, this policy is subject to formal review at least annually (or sooner if prompted by new national legislation, local safeguarding directives, or technical network changes).
- The school will consistently monitor internet traffic, filtering logs, and safety systems. To ensure strategic oversight, the Headteacher, the DSL, and the Online Safety Officer (J. Poston) will review online safety logs weekly.
- The Headteacher will report regularly to the local governing body and the Trust Board on online safety practices, filtering reports, and any logged incidents. Any structural issues or emerging trends will be factored into our safeguarding action plans and curriculum reviews.

## **4. Roles and Responsibilities**

Safeguarding is everyone's responsibility. We adopt a coordinated, whole-school approach to online safety, ensuring all systems operate with the best interests of the child at their heart.

### **4.1 The School's Leadership Team and Swale Academy Trust will:**

- Maintain a strategic, board-level lead for safeguarding to oversee the effectiveness of the school's online safety arrangements.
- Ensure that online safety is treated as a fundamental safeguarding issue, aligned with the Prevent duty, domestic abuse protections, and child-on-child abuse procedures.
- Filter and Monitor Systems (Annual Mandate): Do all that is reasonably possible to limit exposure to online risks by maintaining robust filtering and monitoring systems (Lightspeed).
  - They will review the effectiveness of filters and monitoring systems at least once every academic

year.

- This review must include verified checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a formal written record of these checks must be kept.
- Ensure that online safety is integrated into a progressive, preventative curriculum tailored to the specific developmental stages and vulnerabilities of children (including those with SEND or those who are care-experienced).
- Ensure that all staff, governors, and trustees receive appropriate, updated online safety and safeguarding training at induction and at least annually thereafter. This training must explicitly cover roles and responsibilities in relation to filtering and monitoring.
- Support the DSL, deputy DSLs and the schools' Computing Lead by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Engage with parents and carers about the systems used in school, what children are being asked to do online, and how to maintain safety at home.

#### **4.2 The Designated Safeguarding Lead (DSL) will:**

- Serve as the central point of contact for all online safety and safeguarding concerns, liaising with local authority children's services, the LADO, and Local Police when appropriate.
- Maintain a complete and secure safeguarding picture by working closely with Deputy DSLs, the Computing SLE, the Online Safety Officer, the SENCO, and pastoral leads.
- Ensure they undergo regular training to keep up with the unique risks associated with online safety, including self-generated intimate images and/or videos (including AI-generated content e.g., deepfakes), financial exploitation, online radicalisation, and county lines.
- Understand the specific, heightened vulnerabilities of SEND learners, young carers, and care-experienced children online, ensuring tailored intervention is provided.
- Coordinate active participation in national safety initiatives (such as Safer Internet Day) and lead parental engagement workshops.
- Maintain rigorous, confidential digital records of all online safety concerns and behaviours, using these logs to identify trends and adjust The school's preventative curriculum.
- Ensure that if a pupil leaves the school, their child protection and online safety file is securely transferred to the receiving school within 5 days for an in-year transfer or within 5 days of the start of the next term.

#### **4.3 Members of Staff will:**

- Maintain an attitude of "it could happen here" regarding online abuse, harassment, and exploitation, exercising professional curiosity at all times.
- Adhere strictly to the Swale Academies Trust Acceptable Use of IT Policy, the Staff Behaviour Policy, and professional boundaries.
- Ensure that any internet-derived materials used in the classroom are vetted for age-appropriateness, safety, and copyright compliance.
- Report any online safety concerns, suspicious behaviours, or filtering breaches immediately to the DSL (or deputies) using the school's reporting systems. They must never attempt to investigate or view explicit content themselves.

- Classroom Supervision: Actively supervise learners whenever they are utilising digital technologies in lessons, reinforcing online safety messages dynamically.
- Ensure they complete all mandatory annual online safety training, including understanding their specific role within the school's filtering and monitoring framework.
- Maintain professional boundaries: never contact pupils or parents via personal social media or personal email, and only utilise work-provided accounts and devices for official business.

#### **4.4 Technical Staff and IT Support (Swale Academies Trust) will:**

- Maintain and secure the school's IT infrastructure, ensuring robust firewalls, anti-virus/anti-malware protections, and filtering systems are active.
- Implement the Trust's blocking of unauthorised removable storage (such as USB sticks, memory cards, and external hard drives) on all school computers to prevent malware transmission and unauthorised data extraction.
- Support the leadership team in executing and documenting the mandatory annual filtering and monitoring checks across all internet-connected devices on the premises.
- Ensure all user activity can be monitored and traced to individual login accounts to maintain accountability.
- Report any suspected system breaches, malicious attacks, or critical filtering failures immediately to the DSL, Headteacher, and Trust IT support.

#### **4.5 Learners (commensurate with age and ability) will:**

- Read, sign, and adhere to their age-appropriate Acceptable Use Agreement (AUP).
- Treat peer groups with respect online and offline, recognising that cyberbullying, harassment, and sending abusive messages are entirely unacceptable.
- Take personal responsibility for their safety online: keep passwords secure, never share login credentials, and report any upsetting, offensive or inappropriate material or messages online to a trusted adult.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.

#### **4.6 Parents and Carers will:**

- Partner with the school by reading the Acceptable Use Policy, discussing its contents with their child, and reinforcing safe online habits at home.
- Act as positive online role models, monitoring their children's screen time, device usage, and social media interactions.
- Report any online safety concerns, cyberbullying, or predatory behaviour affecting their child to the school's DSL or the Headteacher.
- Ensure that children do not bring unapproved personal connected devices to school, and respect the school's mobile phone-free environment.

## **5. Education and Engagement Approaches**

### **5.1 Education and Engagement with Learners**

- Preventative education will be tailored to the age, stage, and stage of development of the pupils. It will explicitly cover:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

We will support learners to read and understand the Acceptable Use Policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learners' voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.
- The legal and emotional consequences of creating, possessing, or distributing self-generated intimate images and/or videos (including those generated using AI e.g., deepfakes).
- Media literacy: critical evaluation of online content, validating sources, and recognising the risk of misinformation, disinformation, and fake news.

### **5.2 Vulnerable Learners & Special Educational Needs and Disabilities (SEND)**

- We recognise that children with Special Educational Needs and Disabilities (SEND) or certain medical conditions face additional, disproportionate safeguarding and online safety barriers. These include:
  - High risk of peer isolation and discriminatory or prejudice-based cyberbullying.
  - Cognitive barriers, such as being unable to understand the difference between fact and fiction in online content, leading them to repeat inappropriate behaviours or extreme content without realising the consequences.
  - Communication difficulties, which may hinder them from reporting abuse, grooming, or distress.
  - A heightened susceptibility to online grooming, radicalisation, and financial exploitation due to trust or social vulnerabilities.
  - Dependence on adults for intimate care or physical support, which can blur boundaries.

- The school's SLT, DSL, Computing Lead and any other relevant members will work in close consultation with the SENCO to deliver highly differentiated, ability-appropriate online safety education.
- Differentiated support may include simplified visual guides, highly structured and supervised browsing environments, and the use of assistive communication technologies.
- Young Carers: We explicitly recognise that Young Carers have unique vulnerabilities. Their extensive caring responsibilities can impact their school attendance, mental health, and physical wellbeing, making them more isolated. This isolation can lead to increased and unmonitored online activity. The school will ensure early identification of Young Carers and provide proactive, tailored support to safeguard them online and offline.

### **5.3 Training and Engagement with Staff**

- All new staff (including trainee teachers and volunteers) will receive a comprehensive online safety briefing during their safeguarding induction.
- All staff will complete mandatory annual online safety training. This training is integrated with the wider safeguarding curriculum and covers:
  - Understanding the 4 Cs (Content, Contact, Conduct, Commerce).
  - Recognising the indicators of online abuse, exploitation, grooming, and county lines.
  - Specific expectations and protocols regarding the school's filtering and monitoring systems.
  - Professional conduct expectations on personal social media and the prevention of transferable risk.
  - Staff are reminded that their network usage is logged, monitored, and legally discoverable.

### **5.4 Awareness and Engagement with Parents and Carers**

- The school actively partners with families to keep children safe online. We provide:
  - Regular updates on emerging online safety threats, games, and apps via school newsletters and the school website.
  - Resources detailing what online platforms and tools pupils are utilising in school (e.g., Google Workspace) and how parents can monitor their child's school account safely.
  - An up to date consent for photographs and videos that may be used for school or Trust social media promotional purposes.

## **6. Responding to Online Safety Incidents and Concerns**

### **6.1 Concerns about Learners' Welfare**

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with Local Authority thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

## **6.2 Staff Misuse**

- Any complaint about staff misuse will be referred to the headteacher in accordance with the allegations policy.
- For any allegations regarding a member of staff's online conduct a consultation will be sought with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

## **7. Procedures for Responding to Specific Online Incidents or Concerns**

### **7.1 Child-on-Child Sexual Violence and Sexual Harassment**

- In line with KCSIE 2026 (Part 5), The school recognises that child-on-child sexual violence and sexual harassment can take place online and offline. Staff must maintain a zero-tolerance culture.
- Abusive online behaviours, including grabbing, lewd comments, non-consensual sharing of explicit images, or downplaying harassment as "just banter" or "boys being boys" will be challenged immediately. Failure to challenge these behaviours risks normalising misogyny and creating an unsafe environment.
- Upon receiving a report, the DSL will immediately carry out a comprehensive risk and needs assessment to protect the victim, manage the alleged perpetrator, and safeguard the wider school community.
- Separation in the Classroom: To protect the victim from severe distress and trauma, the alleged perpetrator will be removed from any shared classes with the victim while investigations are conducted. The school will maintain physical separation on the premises, during school-based activities, and on school transport.
- If a criminal offence is suspected, the DSL will immediately contact Local Police and Children's Social Care. The school will co-operate with police investigators to ensure school-level disciplinary actions do not compromise criminal proceedings.

### **7.2 Self-Generated Intimate Images and/or Videos (including those generated using AI e.g., deepfakes)**

- In accordance with KCSIE 2026, the terminology of "youth-produced sexual imagery" has been updated to "self-generated intimate images and/or videos including those generated using AI e.g., deepfakes".
- Taking, sharing, or possessing intimate images/videos of anyone under the age of 18 is a serious safeguarding issue and a criminal offence.
- If such an incident is reported, staff must:
  - NEVER view, share, save, copy, or forward the image or video.
  - Secure and confiscate the device in line with DfE Searching, Screening and Confiscation guidelines.
  - Immediately report the incident to the DSL.
- The DSL will follow the UKCIS Sharing nudes and semi-nudes statutory guidance. This includes conducting a risk assessment, offering pastoral and therapeutic support to all children involved, and Contacting Local Police/MASH.

- Deletion of any content will only take place once the police have explicitly confirmed that it is safe to do so and that no investigation will be compromised.

### **7.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)**

- Online grooming, Child Sexual Exploitation and Child Criminal Exploitation are severe forms of child abuse. Exploitative networks frequently target children online via social media and gaming platforms.
- CCE often involves children being coerced or manipulated into transporting drugs or money through county lines or carrying weapons. The school staff will treat exploited children as victims of modern slavery, ensuring relevant child protection and National Referral Mechanism (NRM) referrals are completed.
- The school will maintain highly visible "Click CEOP" report buttons on the school website and teach pupils how to report suspicious online contact directly.

### **7.4 Indecent Images of Children (IIOC)**

- The school will take all necessary technical precautions (filtering, ISP firewalls) to prevent accidental or deliberate access to Indecent Images of Children (IIOC) on our network.
- Any discovery of IIOC on school-owned or personal devices will result in immediate isolation of the device, referral to Local Police (999/101), the LADO, and the Internet Watch Foundation (IWF) via their online reporting tool.

### **7.5 Cyberbullying**

- Cyberbullying (including prejudice-based, homophobic, transphobic, or racist bullying online) is strictly prohibited.
- Incidents of cyberbullying will be investigated thoroughly under our Anti-Bullying Policy, and disciplinary sanctions will be applied up to and including permanent exclusion. Where cyberbullying involves harassment or threats of physical violence, Local Police can be notified.

### **7.6 Cybercrime**

- Staff will remain alert to the risk of children with advanced computer skills inadvertently or deliberately entering into cyber-dependent crimes (e.g., unauthorised hacking, DDoS attacks, or malware generation).
- If a child is identified as being at risk of committing cyber-dependent offences under the Computer Misuse Act 1990, the DSL will refer them directly to the National Cyber Crime Unit's 'Cyber Choices' preventative programme to redirect their technical skills into positive, lawful pathways.

### **7.7 Online Hate**

- The school promotes an inclusive culture. Any online activity on school networks that promotes hate speech, discrimination, or harassment against protected characteristics is strictly forbidden. Local Police will be consulted if a hate crime is suspected.

## **7.8 Online Radicalisation and Extremism**

- We will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. This is done by using a monitored system and Lightspeed filter.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

## **8. Safer Use of Technology**

### **8.1 Classroom Use**

- Digital technology is utilised across the curriculum to enhance learning.
- Supervision: All pupil access to the internet on-site must be supervised.
  - EYFS and KS1: Internet access is via adult demonstration or strictly controlled, pre-vetted links.
  - Pupils utilise age-appropriate online tools, filtered search engines, and must be guided to pre-checked educational resources.

### **8.2 Managing Internet Access**

- All users must sign their respective Acceptable Use Agreements before being granted network credentials.
- Guests and visitors are permitted to connect to the dedicated Guest Wi-Fi network, which is time-limited and filtered. Staff and pupils are strictly prohibited from connecting personal devices to the main school network.

### **8.3 Filtering and Monitoring (Annual Record Keeping)**

- Lightspeed Filtering: All school-owned devices (Chromebooks, laptops, and PCs) are filtered via Lightspeed. This system actively blocks illegal, inappropriate, or restricted content, including all sites on the IWF blocklist.
- Active Monitoring: This system logs in real-time. Any flagged keywords, search violations, or bypass attempts are immediately sent to the DSL and Computing Lead.
- Device Vetting & Record Keeping: The school's filtering and monitoring configuration is reviewed and verified annually. Technical and safeguarding staff will conduct physical checks across all locations and all categories of devices to ensure there are no loopholes. A written record of these annual checks must be formally kept and signed off by the Headteacher and Safeguarding Governor.

## **8.4 Managing Personal Data Online**

- All processing, storage, and transmission of personal data online will comply with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.
- Personal data (including student progress, addresses, or medical records) must only be accessed on secure, encrypted school networks, and never downloaded to personal or unmanaged devices.

## **8.5 Password Policy and Multi-Factor Authentication (MFA)**

- **Staff Accounts:** All staff are issued unique usernames and passwords. Multi-Factor Authentication (MFA) is mandatory on all staff accounts and must be configured immediately upon account creation. Access to key systems will be restricted until MFA setup is complete. Staff passwords must be changed annually.
- **Learner Accounts:**
  - From KS1, all pupils are provided with unique usernames and passwords. Passwords are set by the Academy Trust and must be kept strictly private.
  - From KS3, all pupils are educated on and encouraged to create their own secure passwords.
- Under no circumstances may any user log in using another person's credentials.

## **8.6 Managing the Safety of the Website**

- The school website is managed securely. The administrator account is protected with strong passwords and MFA.
- No personal contact details, private images, or sensitive personal data of staff or pupils will be published on the website.

## **8.7 Publishing Images and Videos Online**

- Images and videos of pupils may only be published on the school website, official social media, or learning platforms with explicit, written parental consent. No pupil names will be associated with their photographs.

## **8.8 Managing Email**

- All official school business must be conducted using the school-provided email address (@swale.at).
- **MFA & Encryption:** Staff must use MFA for email access. Any attachments containing sensitive or confidential information sent to third parties must be securely encrypted, with passwords verified via an alternative communication channel (e.g., SMS or phone).
- **Removable Storage Block:** In line with Swale Academies Trust rules, all removable storage devices (USB sticks, memory cards, external drives) are blocked on school computers. Staff must utilise Google Drive for file storage, transfers, and collaboration.

## **8.9 Live Stream Lessons for Remote Learning**

- Live-streamed lessons will only occur using platforms approved by the Senior Leadership Team.
- When executing live streams:

- A risk assessment of the platform must be conducted, with chat and recording features disabled where appropriate.
- Where possible, two members of staff must be present in the virtual room. Where this is not possible, the session should be recorded by the school for safeguarding and monitoring purposes.
- Staff must dress professionally, utilise a neutral background, and maintain a professional environment.
- Pupils must be dressed appropriately and participate from a suitable location (not bedrooms).

#### **8.10 Management of Learning Platforms (Google for Education)**

- Google for Education is the official learning platform of the school.
- Access is strictly limited to active pupils, parents, and authorised staff. Accounts are disabled when a user leaves the school.

#### **8.11 Management of Applications (Insight)**

- The school utilises Insight to track student progress and share updates with parents.
- Insight must only be accessed via secure, school-owned devices. Staff are strictly prohibited from installing or accessing the Insight tracking application on personal mobile phones or personal tablets.

#### **8.12 Generative Artificial Intelligence (AI) Tools**

- In line with the DfE safety expectations and KCSIE 2026, the use of Generative AI is captured within this policy under the 4 Cs.
- Staff Usage: Staff are permitted to use Swale-approved AI tools (e.g., Swale-linked Google Gemini and Bromcom AI) for educational drafting, lesson planning, and quiz generation. Staff are strictly prohibited from entering any personal, sensitive, or confidential student/staff data into free or unapproved AI platforms. Personal AI accounts must not be used on school-issued devices.
- Learner Usage: Pupils will be educated on the risks of Generative AI, including deepfakes, copyright infringement, and biased outputs. They will be taught to critically evaluate and validate any AI-generated text or images before accepting their accuracy.

### **9. Social Media**

#### **9.1 Expectations**

- The school expects all members of our community to use social media responsibly. Threatening, defamatory, or inappropriate posts regarding the school, its staff, or pupils will be investigated and may result in disciplinary action or referral to the Police.

#### **9.2 Staff Personal Use of Social Media**

- Staff must not accept "friend" or "follow" requests from current or past pupils on personal social media accounts. Any pre-existing relationships must be declared to the Headteacher and DSL.
- Staff must ensure their privacy settings are set to high and must not post content that brings the teaching profession or the school into disrepute. School email addresses must not be used to

register personal social media accounts.

### **9.3 Learners' Personal Use of Social Media**

- The school actively educates pupils on the age restrictions of popular social media platforms.
- Learners are taught that once a personal image is uploaded to a social media service, that service may retain rights to it, and that Generative AI can be used to manipulate their images maliciously.

### **9.4 Official Use of Social Media**

- The school's official social media pages are risk-assessed and approved by the Headteacher. They are registered using school credentials and managed by authorised administrators.
- Content shared on official channels must comply with data protection laws, image consent registries, and child protection protocols.

## **10. Use of Personal Devices and Mobile Phones**

### **10.1 Expectations**

- The school recognises that mobile technologies are part of modern life but must be regulated to maintain a safe, distraction-free environment.
- The school accepts no responsibility for the loss, theft, or damage of personal devices brought onto school premises.
- Under no circumstances may mobile devices be used in changing rooms, toilets, or poolside areas.

### **10.2 Staff Use of Personal Devices and Mobile Phones**

- Staff must keep their personal mobile phones switched off or on silent and stored securely (e.g., in a desk drawer) during lesson times.
- Staff must NEVER use personal devices to take photographs or videos of pupils. Only school-provided cameras or Chromebooks may be used.
- Staff may utilise personal devices to receive Multi-Factor Authentication (2FA) codes in line with DfE standards, but must not use them to access student records, emails, or personal data.

### **10.3 Learners' Use of Personal Devices and Mobile Phones (Mobile-Free Default)**

- **Mobile-Free Environment:** To align with DfE and Swale Academies Trust standards, The school is a mobile phone-free environment by default. Pupils do not have access to mobile phones or personal connected devices (including smartwatches with cellular/camera features) throughout the school day.
- **Storage Protocol:** If a pupil requires a mobile phone for their journey to/from school, the device must be switched off immediately upon arrival and handed directly to the class teacher at the start of the day. Devices are locked securely and returned to pupils at the end of the day.
- **Breaches:** Any pupil found in possession of an active mobile phone or connected device during the school will have the device confiscated. Confiscated devices will only be released to parents/carers.
- **Searches:** If there is suspicion that a device contains harmful, illegal, or abusive content (such as self-generated intimate images/videos), a search of the device may be carried out by the Headteacher

or DSL, strictly in accordance with DfE Searching, Screening and Confiscation guidelines. If illegal content is suspected, the device will be immediately quarantined and handed to Local Police.

#### **10.4 Visitors' Use of Personal Devices and Mobile Phones**

- Visitors, volunteers, and contractors must keep their mobile phones on silent and out of sight in the presence of pupils.
- Visitors are strictly prohibited from taking photos or videos of pupils on school grounds. Staff will actively challenge and report any visitor violating this rule.

#### **10.5 Officially Provided Mobile Phones and Devices**

- Staff who require communication channels with parents (e.g., for off-site trips) will be issued an official school phone. Official devices must be passcode-protected and used strictly in accordance with our Acceptable Use Policy.

### **11. Useful Links for Education Settings**

#### **Kent Support and Guidance:**

- Swale Education Safeguarding Service. Call: 03000 418 503
- If you are concerned about a child in Kent contact the Front Door on 03000 411111 or [Frontdoor@kent.gov.uk](mailto:Frontdoor@kent.gov.uk)
- Kent Safeguarding Children Multi-Agency Partnership 03000 421126  
[kscmp@kent.gov.uk](mailto:kscmp@kent.gov.uk)

#### **Kent Support and Guidance for Educational Settings:**

- <https://www.kelsi.org.uk/child-protection-and-safeguarding>
- <https://www.theeducationpeople.org/our-expertise/safeguarding/>

#### **Kent Police:**

- [www.kent.police.uk](http://www.kent.police.uk)

For non-urgent police contact 101. If you think the child is in immediate danger, you should call the police on 999.

#### **National Safeguarding & Online Safety Resources:**

- ThinkUKnow (CEOP): [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- National Crime Agency CEOP Safety Centre: [www.ceop.police.uk](http://www.ceop.police.uk)
- Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
- Lucy Faithfull Foundation (Harmful Sexual Behaviour support): [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
- NSPCC Online Safety: [www.nspcc.org.uk/online-safety](http://www.nspcc.org.uk/online-safety)
- Marie Collins Foundation (support for technology-assisted abuse):  
[www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
- UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
- Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
- Cyber Choices (NCA/Preventative programme): [www.nationalcrimeagency.gov.uk/cyber-choice](http://www.nationalcrimeagency.gov.uk/cyber-choice)