ONLINE SAFETY POLICY

October 2026

This policy should be read in conjunction with the following policies and guidance:

Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection Policy. It has regard to KCSIE 2026; the Education (Independent School Standards) Regulations 2026; the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025; the Equality Act 2010; the Human Rights Act 1998; the Computer Misuse Act 1990; the Copyright, Designs and Patents Act 1988; the Online Safety Act 2023; the Prevent Duty Guidance 2023; DfE Filtering and Monitoring Standards updated in 2026; and the Statutory Mobile Phones in Schools Guidance applying from 1 September 2026.

INTRODUCTION

Information and Communication Technology (ICT) in the 21st Century is an essential resource to support learning and teaching and plays an important role in the everyday lives of children, young people and adults. As Christians this is something that we can celebrate and enjoy, and as a school, use to arm our young people with the skills to access life-long learning and employment. We acknowledge that the responsible use of ICT brings great benefits to the school and individuals, however there are risks associated with its use. This document aims to set out Bethany School's policy on the Acceptable Use of ICT including Online Safety, Social Media, and Data Security.

At Bethany School*,* we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

We understand that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk according to KCSIE 2026:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, misandry, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this. For example, child-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm. For example, making, sending, and receiving explicit images, including those generated using AI, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel any of our pupils or staff are at risk, it will be reported.

Internet, mobile and digital technologies cover a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging, and chat rooms
- Social Media platforms and services
- Mobile/ Smart phones with text, video and/ or web functionality

- Other mobile devices including tablets and gaming devices and smart watches
- Online Games
- School approved learning platforms and online learning services
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements.

The School holds personal data on learners, staff, and others to help conduct day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreements (for Staff, Volunteers, Governors and Pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

ONLINE SAFETY ROLES AND RESPONSIBILITIES

Governors

As Online Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Online Safety Coordinator

Mr David Charles (Designated Safeguarding Lead) is the Online Safety Coordinator for Bethany School. It is the role of the Online Safety Coordinator to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and Governors are updated by the online safety Safeguarding Officer and all Governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

All staff

All members of the school community have been made aware of who holds this post. However, it should be clear to all staff that Online Safety and the handling of secured data is everyone's responsibility.

DATA PROTECTION

DISINFORMATION, MISINFORMATION, AND HARMFUL CONTENT

Pupils may be exposed to false or misleading content online, including conspiracy theories, political misinformation, health-related disinformation, or extremist narratives. The school recognises this as a safeguarding risk. Staff will be trained to identify signs that a pupil may be affected by such content and respond appropriately. Digital literacy and critical thinking are embedded in the curriculum to help children challenge and question information responsibly. Where such exposure presents a risk of radicalisation or emotional harm, staff will follow safeguarding and Prevent referral procedures.

CYBERCRIME

Cybercrime is criminal activity committed using computers and/or the internet. It may be **cyber-enabled**, where technology increases the scale or speed of an offence that could also occur offline, or **cyber-dependent**, where the offence can only be committed using a computer or network.

Cyber-dependent offences may include unauthorised access to computers or networks, denial-of-service attacks, and creating, supplying or obtaining malware or other tools for use in cybercrime. Staff should be aware that children with particular skills or interests in computing and technology may become involved in illegal online activity without fully understanding the legal, ethical or safeguarding implications.

Any concerns about a pupil becoming involved in cybercrime should be reported to the Designated Safeguarding Lead or deputy. Where appropriate, the DSL should consider referral to the **Cyber Choices Programme**, a preventative police programme which aims to divert young people who are at risk of becoming involved in low-level cyber-dependent offending towards positive uses of their skills and interests. Normal safeguarding procedures should also be followed where there are concerns about exploitation, coercion or harm.

ONLINE SAFETY, FILTERING MONITORING, AND AI-RELATED RISKS

The school uses appropriate filtering and monitoring systems to protect pupils from illegal, inappropriate and harmful online content. In line with KCSIE 2026 and the DfE Filtering and Monitoring core standard updated in 2026, roles and responsibilities are clearly assigned, safeguarding alerts are acted upon promptly, and provision is reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support. Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks. The review will consider whether systems can respond appropriately to dynamic, personalised and AI-generated content.

Appropriate filtering and monitoring technology on school devices and school networks form part of our online safety. We ensure we have effective monitoring strategies in place that meet our safeguarding needs.

- Our school's filtering and monitoring technology is the responsibility of David Charles in conjunction with Datamills Ltd who is the school's Network Manager.
- IT use is monitored using the following filtering and monitoring system: Cisco Umbrella

The school will review its overall approach to online safety at least annually, including filtering and monitoring provision. This review will be supported by an annual risk assessment which considers and reflects the online risks faced by the school's pupils, including emerging risks associated with new technologies and generative AI.

The school will block harmful and inappropriate content without unreasonably impacting teaching and learning.

Our Governing Body reviews the standards and discusses with IT staff and service providers what more needs to be done to support the school in meeting this standard.

- IT use is monitored using the 'cisco umbrella' filtering and monitoring system to ensure that pupils are protected from harmful content.The system logs user activity for safeguarding purposes.
- ICT equipment owned or leased by the school may be inspected at any time without prior notice on the authorisation of the Head Teacher.
- Authorised ICT consultants, Datamills UK may monitor and inspect all internet activities which make use of the Bethany School server at any time. Personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards, and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

Monitoring, interception and access to communications will be lawful, necessary, proportionate and transparent, and will comply with current data protection law, the Human Rights Act 1998 and applicable

communications legislation, including the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 where relevant. Monitoring will be undertaken only for legitimate school purposes and with appropriate governance and safeguards.

BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of permission to use school ICT hardware, software or services for a specified period.

For staff, any policy breach is grounds for disciplinary action in accordance with the Staff Code of Conduct and may lead to disciplinary action.

The Information Commissioner has regulatory and enforcement powers under current data protection law. The school will manage personal-data breaches and regulatory obligations in accordance with its Data Protection Policy and current ICO guidance.

For pupils, reference will be made to the school's Good Behaviour and Discipline Policy and include reporting the breach to the Head Teacher who may consider a period of exclusion. The Head Teacher may refer the matter to Governors who may take further action.

INCIDENT REPORTING

See Appendix B "Response to an Incident of Concern". An 'incident' is taken to mean any event which contravenes the "ICT Acceptable Use Agreement". These include any security breaches or attempts, loss of equipment or PINs, virus notifications, unsolicited emails, data breaches and any unauthorised use of or suspected misuse of the internet, or mobile and digital technologies such as accessing inappropriate material, or misuse of emails.

Any incident must be immediately reported to the School's Relevant Responsible Person (Mr David Charles).

Some incidents may need to be recorded if they relate to bullying, extremism or racist behaviour. This will be via our Incident or Anti-bullying log and will take into account our Safeguarding, Prevent Strategy, Anti-bullying and Good Behaviour and Discipline Policies.

Please refer to the relevant section on **Incident Reporting and Recording.**

COMPUTER VIRUSES

All files downloaded from the Internet, received via e-mail or on removable media such as a USB storage device or other removable media must be checked for any viruses before being used.

Never interfere with any security or endpoint-protection software installed on school ICT equipment.

If your machine is not routinely connected to the school network, you must make provision for regular security updates.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

DATA SECURITY AND ICT ACCEPTABLE USE

The accessing and appropriate use of school data is something that Bethany School takes very seriously with reference to GDPR regulations and Data protection in schools - Guidance - GOV.UK

An Information Asset Register is held which enables us to be aware of what information is stored and for what purposes, as well as how it needs to be protected, how information will be amended or added to over time, who has access to data and why and how information is retained and disposed of. (See Data Protection Policy for more details about the relevant responsible people for data protection).

The school gives relevant staff access to its ICT network when they have been issued with guidance and training and have signed the **ICT Acceptable Use Agreement** to demonstrate that they have understood the school's Online Safety Policy and Data Security issues. See Appendix A for ICT acceptable use agreements.

All staff are issued with a unique username and password which must always be used and must not be disclosed to others (except authorised ICT staff when required).

It is the responsibility of everyone to keep passwords secure and inform the head teacher immediately if there is a breach of security with password or account information.

Personal data must not be downloaded onto storage devices or laptops.

All staff are responsible for keeping school related data secure. This includes all personal, sensitive, confidential or classified data used in school or, when relevant, taken out of school. Staff should be careful with mobile ICT equipment and printed data, especially using shared printers/copiers. They should use the 'delay print function' when printing sensitive data from a device located away from the printer. They should also be aware of sensitive information which may be seen if left open on an unprotected computer screen.

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

An appropriate secure data-erasure method will be used for all redundant ICT equipment that may have held personal data to ensure the data is irretrievably destroyed, or if the storage media has failed, it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2013
- Data Protection Act 2018

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

Further information available at:

- The Waste Electrical and Electronic Equipment Regulations 2013
- https://ico.org.uk/
- Data Protection Act 2018

ONLINE/VIRTUAL TEACHING

If the school needs to use online or virtual teaching the school will:

- ensure all relevant staff are briefed so they understand the policies and the standards of conduct expected of them.
- consider any advice published by the local authority, or their online safety / monitoring software provider. Such as setting clearly defined operating times, senior staff able to 'drop in' on lessons at any time, regular contact with parents, possibility of using alternatives such as pre-recorded lessons.

Whilst using online or virtual teaching staff should adhere to all the usual safeguarding and online safety practices and procedures.

This means that adults should **not**:

- contact pupils outside the operating times defined by the Headteacher
- take or record images of pupils for their personal use.

- record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff).
- engage online while children are in a state of undress or semi-undress.

It is the responsibility of the staff member to raise any issues of suitability (of dress, setting, behaviour) with the child and/or parent immediately and end the online interaction if necessary.

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues, e.g., whether parental/pupil consent is needed and retention or storage.

EMAIL

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsible online.

MANAGING EMAIL

The school gives all staff & Governors their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. Personal email addresses should not be used to contact staff, pupils, parents or conduct any school business.

- Each account holder is responsible for keeping passwords secure
- Email should be used responsibly and checked regularly.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- For the safety and security of users and recipients, all mail is filtered and logged, if necessary, email histories can be traced.
- Emails created or received as part of school business are school records and must be managed in accordance with the schools data protection policy and records-retention arrangements. Therefore, email accounts must be actively managed as follows:
    - Delete all emails of short-term value.
    - Carry out frequent housekeeping on all folders and archives
- Attachments from an untrusted source should never be opened;
- Staff must inform the Head Teacher if they receive an offensive email
- Pupils are introduced to email as part of ICT lessons, Tutor Time and particularly during Communication Topic.
- Pupils may access their own email account at certain times during school, but are expected to behave responsibly, in line with the ICT Acceptable Use Agreement.
- Pupils in Y6-Y11 are issued with School email addresses for educational purposes. These accounts will be deleted when the pupil leaves Bethany School.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email

EMAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

Emailing sensitive, confidential or classified information is discouraged, however where your conclusion is that email must be used to transmit such data you must liaise with your Head Teacher and exercise caution when sending the email. Documents of this nature should be sent to no more recipients than necessary, as a password protected attachment and details/receipt verified by phone or email. The password must be provided by separate contact with the recipient. Often posting or hand delivering such documents is preferred.

INTERNET USE AND ONLINE SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum, and we continually look for new opportunities to promote online safety.

See Teaching online safety in schools - GOV.UK

and Education for a Connected World - GOV.UK

In accordance with KCSIE, Bethany school will review its approach to online safety every year using an online safety audit tool such as LGFL online safety audit OS Audit - Online Safety Audit from LGfL | LGFL or Online Safety

Pupils are taught online safety, computing, ICT, use of email, and internet use throughout the school curriculum including in tutor time, ICT lessons, communication topic and worldview studies as well as ad hoc reminders as the opportunity arises. See curriculum grids for more information.

Online safety curriculum content includes.

- Accessing designated websites under supervision, with permission (for pre checked, designated sites) or independently (for senior age pupils when the Acceptable Use Agreement has been signed.)
- Educating pupils about the online risks that they may encounter outside school in an age-appropriate manner informally in an ad-hoc manner whenever opportunities arise.
- Reception and Y1 consider online safety in PSHE. Pupils in Y2 upwards have Online Safety lessons in their computing lessons or tutor time at the start of the academic year. Junior pupils use the 'Internet Legends' internet safety course from Google and Purple Mash resources, and Secondary pupils will complete an individual certificate of online safety via Online Safety Alliance in the senior class and then again in the GCSE class. This is up to date and addresses all current issues in line with 'Education for a Connected World'. Pupils in Year 6 upwards will be expected to sign the ICT Acceptable Use Agreement each year, and are taught and regularly reminded of its contents during tutor time and via poster displays
- Pupils are taught about copyright, respecting other people's information, safe use of images and not sharing personal details through discussion, modelling and appropriate activities within the classroom
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Pupils may be exposed to fake or misleading content online, including conspiracy theories, mis-information and disinformation or extremism. They are taught to critically evaluate materials and learn good searching skills throughout the curriculum to help them question information responsibly.
- Online Safety advice is promoted widely through school displays, posters and class activities such as Safer Internet Day in February.
- Some aspects of Online Safety are covered when every Year 6 group attends the "Crucial Crew" event run by South Yorkshire Police.

EQUAL OPPORTUNITIES: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils however, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of Online-Safety. Internet activities should be planned and well managed for these children and young people.

Updates - Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK

ONLINE SAFETY SKILLS DEVELOPMENT FOR STAFF

New staff receive information on the School's Online Safety policy and ICT Acceptable Use Agreement as part of their induction. Some primary staff have completed the 'Internet Legends' training course provided by Google and all staff access annual training from Online Safety Alliance.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (report to the Head Teacher). As this policy is reviewed, staff are made aware of changes and are regularly reminded of their responsibilities.

All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern at regular staff meetings.

INCIDENT REPORTING AND RECORDING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Online Safety Coordinator. Additionally, all security breaches, lost/stolen equipment, or data (including remote-access credentials and authentication information), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

Some incidents may need to be recorded if they relate to bullying, extremism or racist behaviour. This will be via our Incident or Anti-bullying log and will take into account our Safeguarding, Prevent Strategy, Anti-bullying and Good Behaviour and Discipline Policies.

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. If staff or pupils discover an unsuitable site, the **screen** must be switched off/ closed and the incident reported immediately to the Head Teacher, or teacher as appropriate

- Deliberate access to inappropriate materials by any user will lead to the incident being logged and an investigation by the Head Teacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of the LADO and police for very serious offences

- Users are made aware of sanctions relating to misuse or misconduct in the code of conduct and safeguarding policies.

- Please see Appendix E regarding how to respond to an incident involving a **nude or semi-nude image** of a child/pupil. **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**. If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
  Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK

MANAGING OTHER ONLINE ISSUES

Online technologies (including social networking sites and games, if used responsibly) can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some **content, contact, culture, and commerce**. (The four areas of online safety risk, KCSIE) To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services, software, and apps before use.

- Staff members should not ask pupils to sign up to online games, sites or services that have an inappropriate user age
- All pupils are required to keep their mobile phones switched off and in their bags whilst on the school premises
- Smart Watches should be set to 'Do Not Disturb' Mode
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile or home phone numbers, school details, email address, specific hobbies and interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Services such as Facebook, Instagram, WhatsApp etc have a 13+ age rating which should not be ignored https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services
- On-line gambling or gaming is not allowed.

Please see our "Social Media Responsible Use Guidelines" in Appendix C which give more detailed advice about using good judgement and being respectful and responsible when representing Bethany School in Social Media Spaces

PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting Online-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss Online-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain, specifically in printed material, display material, school website, Bethany School public Facebook page, parents and teachers Facebook page, and the class dojo (if used). They are also expected to adhere to the decision made by other parents in this regard and not assume that consent has been given.

- Parents/carers of Y6 and Senior/GCSE pupils are expected to sign The Pupil ICT Acceptable Use Agreement with their children

- Volunteer helpers are expected to sign the Staff/Governors/Volunteers ICT Acceptable Use Agreement

- Bethany School disseminates information to parents relating to online safety where appropriate through:

    - Parents meetings
    - Practical training sessions e.g. current online safety issues, and online safety training for parents from Online Safety Alliance.
    - Monthly email newsletters from 'Knowsley City Learning Centres' Online Safety - Knowsley City Learning Centres

DORMANT AND UNUSED ACCOUNTS

Accounts belonging to users who have left the school or who no longer require access must be disabled promptly to prevent unauthorised access.

PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

Personal, sensitive or confidential information must be processed in accordance with the schools data

protection policy

- Ensure that any school information accessed from a personal PC or removable media equipment is kept secure and any portable media is removed from computers when not attended.
- Ensure screens are locked before moving away from computers during a normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential, and classified information that is disclosed or shared with others.
- Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential, and classified information contained in documents that are copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used.
- Only download personal data from systems if expressly authorised to do so
- Personal, sensitive, confidential, or classified information must not be posted on the internet, or such information disseminated in any way that may compromise its intended restricted audience.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Hard copies of data must be securely stored and disposed of after use in accordance with the document labelling.

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Removable media should be purchased with encryption.
- All removable media must be stored securely.
- All removable media that may hold personal data must be securely disposed of.
- All files containing personal, sensitive, confidential, or classified data must be encrypted.
- Hard drives from machines no longer in service must be removed and stored securely or wiped clean.

Guidance on How to Encrypt Files can be found on the ICO website: Encryption and data storage | ICO

REMOTE ACCESS

- Staff are responsible for all activity carried out using their remote-access credentials
- Remote access to school systems must use school-approved secure methods and devices and must be protected by appropriate authentication, including multi-factor authentication where required
- Remote-access credentials, authentication codes and other security information must be kept confidential and must not be shared
- Remote access should only be enabled for authorised users where it is required and should be disabled when no longer needed. Where appropriate, a secure virtual private network (VPN) or other approved encrypted connection should be used
- School information and data must remain protected when accessed remotely, particularly when using networks or devices outside the school.

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

The following applies to all parts of the school including the Early Years and Reception class.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. Guidance can be found at:

https://www.safeguardingsheffieldchildren.org/assets/d504ee07/personal_electronic_devices_photographs_and_images_sept_23.pdf

With the written consent of parents (on behalf of pupils) and staff, the school permits staff members to take appropriate images of pupils with school equipment and, in exceptional circumstances, on personal devices. If images are taken on personal devices, they should be quickly uploaded onto the school system and deleted from the device. Pupils and staff must have permission from the Head Teacher before any image can be uploaded for publication.

Parents, carers or spectators may usually take photographs/film events for personal use (unless instructions are given not to do so) and are expected to abide by social media guidance in not sharing on social media, or gaining permission from children, their parents and carers before sharing photographs and videos that include them. Parents and carers may talk to the Head Teacher if they have any concerns about images being shared.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the appropriate teacher. Pupils and staff must have permission from the Head Teacher before any image can be uploaded for publication.

Bethany school acknowledges that some families and staff members know each other personally outside of the school setting through church or other friendship groups. Some staff members also attend family afternoons with their children as 'parents' rather than 'employed' school staff and as such may have cause to use their personal device to take images. In this circumstance the usual parent guidance applies regarding taking and sharing images. Staff members should act with caution to protect themselves from allegations of misconduct.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

Permission to use images of all staff who work at the school is sought as needed.

PUBLISHING PUPIL'S IMAGES

On a child's entry to the School, all parents/carers will be asked to give permission to use their child's images in the following ways:

- on the School website
- in the School prospectus and other printed publications.
- in display material that may be used within the School.
- on the School's public Facebook page
- on the School's private "parents and teachers Facebook page"
- on the class dojo app where used

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Before posting student images online, or using in display or other educational purposes, a check needs to be made to ensure that permission has been given.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the School.

Pupils' full names will not be published alongside their image. Email and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting images or work on the Internet, a check needs to be made to ensure that full names and identifying details are **not** included along with the image.

Further information relating to issues associated with school websites and the safe use of images in schools may be found at: Data protection and school websites - Hertfordshire Grid for Learning

STORAGE OF IMAGES

In line with GDPR, images are used only with the written consent of the parent/carer, which is secured in the first instance on a child's entry to school. Records are kept on file and consent can be changed by parents/carers at any time.

In the Early Years and Primary setting, additional consent is gained for images that are taken on the classroom tablet/school device and are uploaded to class dojo which is a communication tool shared with class parents. The class teacher has the responsibility of deleting the images from the class dojo and the tablet regularly, and when the pupil has left the School.

Images/ films of children are stored securely on the school's network and deleted once the pupils have left unless consent is gained to use the image, e.g. in publicity material. Bethany school holds an archive for appropriate storage of older photos and documents.

Pupils and staff are not permitted to use personal portable media for storage of images.

WEBCAMS and VIDEO CONFERENCING

- We do not use publicly accessible webcams in school.
- Permission will be sought from parents and carers if their children are involved in video conferences or video recordings with endpoints outside of the school.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Webcams include any camera on an electronic device which is capable of producing video.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as smartphones, tablets, and gaming devices are generally very familiar to children outside of school. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING MOBILE PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- The school operates as a mobile-phone-free environment by default throughout the school day, in line with statutory DfE guidance. Pupils are allowed to bring personal mobile devices/phones to school but must not use them on school premises at any time during the school day, including break times and before and after school. Mobile phones must be switched off and kept in a pupil's bag, phones seen out during the school day will be confiscated. Occasionally pupils may be given permission to use mobile phones for research purposes with the express permission of their class teacher, although use of school devices is preferred.
- Pupils participating in Private study may be asked to hand in mobile phones at the beginning of the lesson.
- Smart watches must be set to 'Do not disturb' mode
- School staff wearing smart watches should set devices to 'Do not disturb' or 'school mode'
- All adults in school (teachers, volunteers, parent helpers etc.) are encouraged to demonstrate good practice by not using their own mobile phone for personal reasons in front of the children. There may be occasions where it is appropriate for an adult to use a mobile phone or similar device, for instance calling for assistance or using multi-factor authentication.
- The school is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Never use a hand-held mobile phone whilst driving a vehicle.
- The School has a digital camera, tablet and mobile telephone which is available for use by staff during off site School trips for making calls and taking photos which can then be uploaded to the School system.

SOCIAL MEDIA

See Appendix C for social media guidelines.

Facebook, X (formerly Twitter), Instagram and other forms of social media are increasingly becoming an important part of our daily lives.Staff, Governors, pupils, parents, and carers are aware that the information, comments, images, and videos they post online can be viewed by others, copied, and stay online forever and may form part of pre-employment checks.

Staff, Governors, pupils, parents, and carers are aware that their online behaviour should always be compatible with UK law.

We use images of families, work and pupils from time to time to publicise our School on our Facebook page and website, when appropriate consent has been obtained. Families may change their consent at any time and ask for images to be removed if desired.

Our School also uses an informal 'parents and teachers' Facebook page and a School WhatsApp group to communicate with parents and carers. Any parent/staff member is able to post messages to each other and is expected to behave in a respectful and responsible manner in this setting.

The following information is listed on the Facebook group, as part of the group description and is re-posted from time-to-time as a reminder to all parents.

> "I have added you on to the Bethany parents and teachers Facebook group. It's a closed group for us only and we use it for informal reminders, support, requests and sharing information etc. Photos and posts are shared privately within this group on the understanding that they are not re-posted or shared externally without permission from those concerned. Users should be aware that not all pupils have given consent for their images to be posted to this group. They should be considerate of others' wishes in this regard, and only post images to this group if certain that consent has been given. Families may change their consent at any time and ask for images to be removed if desired. We recommend that people check the privacy settings of their social media account to understand who else will be able to view any images they share.
>
> Seek advice from admin if you are not sure, or ask permission directly."

A similar message is shared in the WhatsApp group which is not used for sharing photos of children. .

SERVERS

The Bethany School Server is located in a secure room, accessed by authorised staff only, and all data is regularly backed up off site and on an additional hard drive by Datamills UK according to the following guidelines.

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly.
- Backups must be encrypted where appropriate and stored securely, with appropriate off-site or logically separate backup arrangements.

WRITING AND REVIEWING THIS POLICY

REVIEW PROCEDURE

There will be on-going opportunities for staff to discuss with the Online-Safety coordinator any Online-Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the DPO any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration will be given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted, or the Central Government changes the orders or guidance in any way.

This policy has been read, amended, and approved by the staff, Headteacher and Governors

Policy agreed by Governors - October 2026

Policy due for Review - October 2027

Bethany School Pupil ICT Acceptable Use Agreement Online Safety Rules

Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device, as you would face to face.

‘So in everything, do to others what you would have them do to you’ Matthew 7v12

- I will only use school ICT and my school email address for school purposes
- I will not download or install software on school technologies
- I will only open email attachments from people I know, or who my teacher has approved
- I will only log on to the school network using my own username and password and will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with pupils, teachers or others is responsible, polite and sensible
- I will not look for, save or send anything that is unpleasant, offensive, or illegal. If I accidentally find anything like this I will report it to my teacher immediately
- I will not give out any personal information such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher
- I am aware that if I take images or video of pupils and/or staff in school that I must only store and use these for school purposes and must never distribute or ‘share’ images without the permission of all parties involved. I will not upload any video, images, sounds or text that could upset any member of the school community including with the use of AI.
- I will be responsible for my behaviour when using ICT and will try to ensure that my online activity both in school and outside school will not cause distress to others or bring the school community into disrepute.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not attempt to bypass the internet filtering system
- I will not sign up to online services until I am old enough to do so
- I will take due care with all school ICT equipment
- I will respect the privacy and ownership of others’ work online at all times
- I am aware that the school policy is for mobile phones to be kept out of sight and switched off at all times on school premises, and that breaking this rule will result in school sanctions
- I am aware that smart watches must be set to ‘do not disturb’ mode and that inappropriate use of a smart watch will result in school sanctions
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted

Bethany School Pupil ICT Acceptable Use Agreement and Online Safety Rules

Dear Parent/Carer

ICT, including the internet, e-mail, and mobile technologies is an important part of learning in our school. We expect all children to be safe and responsible when using ICT.

The Online Safety Rules (see over page) have been discussed with your child in School. Please re-read and discuss these Online Safety rules with your child, and return the slip at the bottom of this page to their class teacher. This agreement outlines both your own, and your child's willingness to support the Schools approach to ICT. If you have any concerns or would like some further explanation please contact Mr David Charles and/or refer to the Online Safety Policy that can be found in the policies section of the school website.

Bethany school endeavours to take every reasonable precaution to ensure that our pupils are safe when using the internet. Please take care to ensure that appropriate systems are also in place at home to protect and support your child/ren. You will find help with this in the online safety newsletter that is circulated via email each month.

✂

Parent Agreement

This document has been discussed with ……. (Child's name) at home.
I give permission for my child to have access to the internet and ICT systems at school, and be given their own email address for use with Google classroom.
I agree to support the safe use of ICT at Bethany School by helping my child to follow the rules overleaf.
I understand the school's policy is that pupils should not sign up to services such as Facebook, Instagram, Snapchat, Tiktok, WhatsApp, X (formerly Twitter) and YouTube whilst they are under age, (13+ years in most cases).
I will behave responsibly and respectfully in my own online activity, ensuring that it does not bring the school community into disrepute.

Parent/ Carer Signature …… **Date**…….

Pupil Agreement

I have discussed the rules overleaf in class and with my parent/carer and agree to abide by them. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

Pupil Signature……**Class** …… **Date**……

Bethany School Staff/Governor/Volunteer Acceptable Use Agreement and Online Safety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities, can stay safe online and protect the schools system and data when using any form of ICT. All staff and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr David Charles.

- I understand that the school digital technology systems are intended for educational use within the policies and rules set down by the school
- I will communicate with pupils, parents and other staff using official school systems for school related business.
- I will comply with ICT and 'Google for Education' security settings such as 2 factor authentication, 6 character pin codes, secure passwords, and not disclosing passwords to others.
- I will ensure that all electronic communications with pupils and staff are respectful and compatible with my professional role
- I will use the staff WhatsApp group appropriately, not for reporting or discussing sensitive pupil information and not for sharing images/videos
- I will use the parent/staff Facebook group appropriately, only sharing images/videos with the required consent
- I will follow requirements for data protection as outlined in the online safety and data protection policies to ensure that personal data is kept secure and is used appropriately, whether in School, taken off the school premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head Teacher
- I will not browse, download, upload or distribute any material that is illegal
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of to the appropriate person
- Images of pupils and/or staff/Governors will only be taken, stored and used for professional purposes in line with School policy and with written consent of the parent, carer, Governor or staff member. I will not use personal equipment to take/record images without permission.
- Images will not be distributed outside the School network without the permission of the parent/ carer, Governor, member of staff or Head Teacher and it will not be possible to identify by name, or other personal information those who are featured.
- I understand that all my use of the Internet and other related technologies using school systems can be monitored and logged and can be made available, on request, to my Head Teacher
- I will respect copyright and intellectual property rights and will not access other users files without permission
- I will ensure that my online activity, both in School and outside School, is responsible and respectful and will not bring the School, my professional reputation, or the school community into disrepute
- I will support and promote the School's Safeguarding, Online Safety and Data protection policies and help pupils to be safe and responsible in their use of ICT and related technologies
- When using my own mobile device to access school data I will follow the rules set out in the agreement and I will ensure that such devices are protected by up to date software and secure passwords, and ensure that I log out of shared devices to keep data secure and will not download data onto my own device.
- I will support the schools policy on mobile device use by minimising my own use of mobile phone in school and setting smart watches to 'do not disturb/school mode'

User Signature

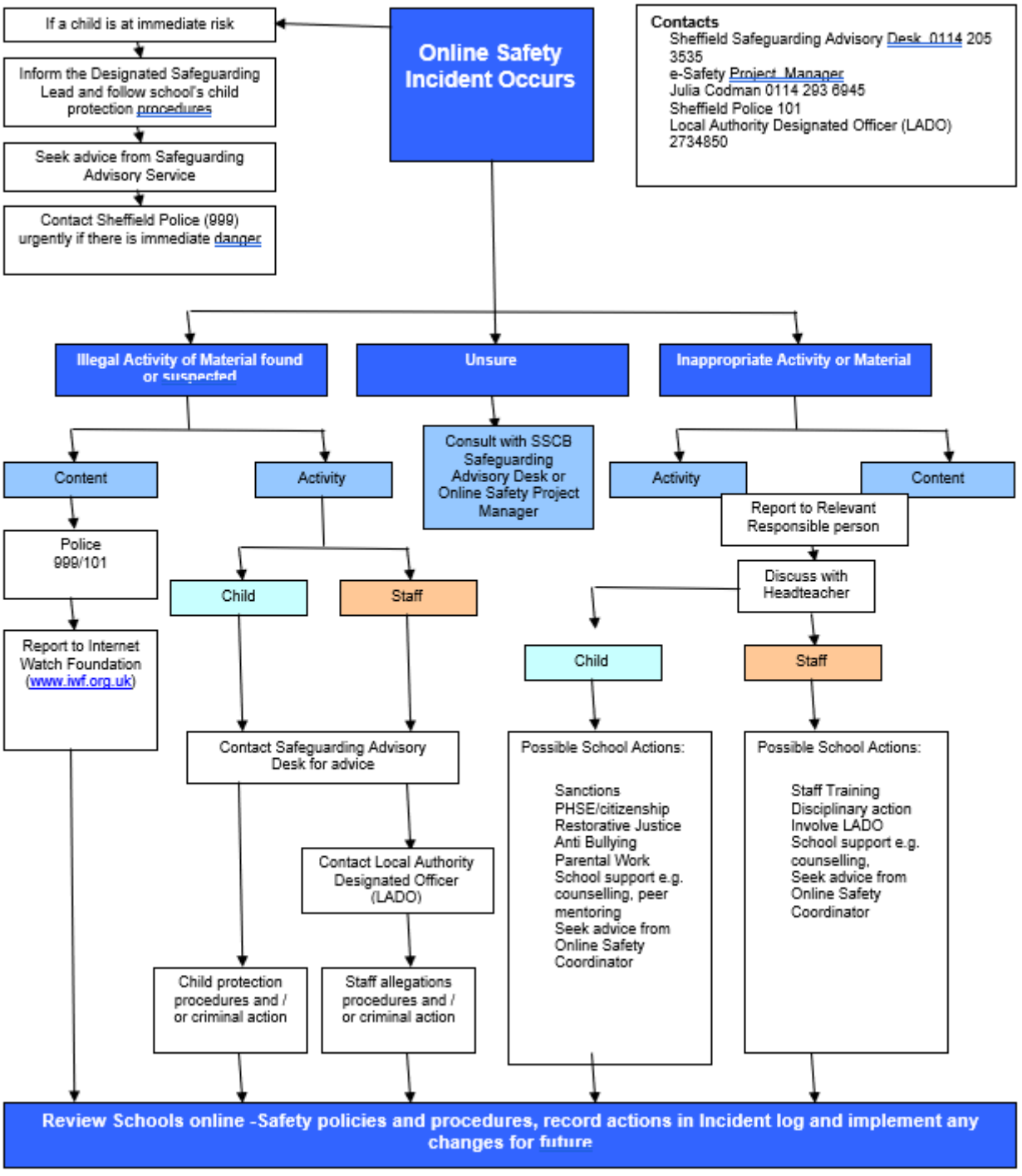
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School

Signature …….…….…… Date ……

Full Name ……..... (Printed)

Job title ……

Appendix B
Response to an Incident of Concern



Appendix C

Bethany School Social Media Responsible Use Guidelines

At Bethany School, teachers, pupils, staff, Governors and parents can use social networking/media as a way to connect with others, share resources, create educational content, enhance the classroom experience, and network within and outside of the School community. While social networking is fun and valuable, there are some risks we need to keep in mind when using these tools. In the social media world, the lines are often blurred between what is public or private, personal or professional.

Social media refers to online tools and services that allow any Internet user to create and publish content. Many of these sites use personal profiles where users post information about themselves. Social media allows those with common interests to share content easily, expanding the reach of their ideas and work. Popular social media tools include Facebook, X (formerly Twitter), LinkedIn, Instagram, YouTube and Flickr to name a few. Below are guidelines to follow when we are representing Bethany School in social media spaces, regardless of whether these are considered professional or personal spaces.

Use good judgement

We expect good judgement in all situations. Behave in a way that will make you and others proud and reflect well on our School.
Know and follow the School's key values of Respect and Responsibility and our ICT Acceptable Use Agreement.
Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

Be respectful
Always treat others in a respectful, positive, and considerate manner.

Be responsible and ethical
Because you represent the School, please stick to discussing only those School-related matters that are within your area of responsibility.
Adults should be open about their affiliation with the School and the role/position they hold.
Share and interact in a way that will enhance your reputation, the reputation of others, and the reputation of the School, rather than damage them.
If you are someone's peer, interact with them online if you are so inclined. If you are a teaching staff member thinking about interacting with a pupil, you must not use social media, but use your School email account and only contact the pupil regarding official School matters.

Be accurate and appropriate
Check all work for correct use of grammar and spelling before posting.
A significant part of the interaction on blogs, X (formerly Twitter), Facebook, and other social networks involves passing on interesting content or sharing links to helpful resources. However, never blindly repost a link without looking at the content first

Be a good listener
Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly, and share feedback.
Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback.

And if you don't get it right……
Be sure to correct any mistake you make immediately, and make it clear what you've done to fix the mistake.
Apologise for the mistake if the situation warrants it.
If it's a major mistake or data breach (e.g., exposing private information or reporting confidential information), please tell the Head Teacher immediately so the School can take the proper steps to help minimise the impact it may have.

Be confidential
Do not publish, post, or release information that is confidential or private. Online “conversations” are never private.

Respect private and personal information

- To ensure your safety, be careful about the type and amount of personal information you provide.
- Avoid talking about personal schedules or situations.
- Never share or transmit personal information of pupils, parents, staff, Governors or colleagues online.
- While taking care when posting to safeguard people’s privacy, be sure – as necessary and appropriate – to give proper credit to sources. In cases of doubt, privacy should be the default.
- Generally use only first names.
- Post images with care
- Respect brand, trademark, copyright information and/or images of the school.
- Do not caption photos with the names of pupils.
- Do not post photos of pupils who have not given consent to do so. (Ask your teacher or see the Head Teacher for details.)

Responding to negative feedback
If someone posts a critique about Bethany School on social media, we hope that a member of our community would respond to the comment in a positive way. The first step is to inform the Head Teacher so the situation can be monitored. The next step is to make contact offline and respond to the comment in a positive way. Our third step would be to have the School respond in an official capacity and if appropriate, suggest a meeting in person to address the issue mentioned in the comment.
If the comment includes profanity, hate speech, or verbally attacks a specific person or group, we delete the comment immediately. Our rationale is that a comment of this sort goes against our view of Responsibility and of Respect and will not be part of Bethany School.

Community of Respect
The most essential standard of appropriate behaviour is that all members of the community will treat one another with kindness, honour, and respect in all situations.

APPENDIX D- HELP AND SUPPORT

Useful Links
Sheffield Safeguarding Partnership Website : Sheffield Children Safeguarding Partnership - Resources
Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK
Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

The Information Management Toolkit for Schools is available at:
https://irms.org.uk/general/custom.asp?page=SchoolsToolkit

Safeguarding Children online – free expert advice: http://www.getsafeonline.org

Review Online e-Safety Policy and practice at https://360safe.org.uk/

Resources to support schools with online safety:
Education for a Connected World – 2020 edition

PSHE Association

Parent Zone

Keeping Children Safe in Education 2026 – GOV.UK

Mobile phones in schools - GOV.UK

Appendix E
SHARING NUDES AND SEMI-NUDES POLICY

Including consensual and non-consensual making or sharing of nudes and semi-nudes, including AI-generated and digitally manipulated images

This policy should be read alongside the school's Safeguarding and Child Protection Policy, Online Safety Policy, Behaviour Policy and any Searching and Confiscation Policy or procedures.

This policy has regard to Keeping Children Safe in Education 2026 (KCSIE 2026) and the UK Council for Internet Safety (UKCIS) guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people, updated March 2024.
New UKCIS Guidance: Sharing Nudes and Semi-Nudes - Safer Schools

INTRODUCTION

KCSIE 2026 refers to consensual and non-consensual making or sharing of nudes and semi-nudes, including those generated using artificial intelligence (AI).

For the purposes of this policy, making or sharing nudes and semi-nudes means the creation, sending or posting of nude or semi-nude images by young people under the age of 18. Images include photographs, videos and livestreams and may be shared online, through apps, social media, gaming platforms or messaging services, or directly between devices.

The term 'nudes' is used because it is widely understood by young people and captures the range of image-sharing behaviours covered by current guidance. Images may be taken by the child themselves, taken or created by another person, digitally altered, or wholly generated using AI, including so-called deepfakes or deep nudes.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. Such images may be created and shared consensually by young people who are in relationships, as well as between those who are not in a relationship. It is also possible for a young person in a consensual relationship to be coerced into sharing an image with their partner.

Incidents may also occur where:

- children and young people find nude and semi-nude images online and share them claiming to be from a peer
- children and young people digitally manipulate, create or alter an image of a young person, including through AI or deepfake technology.
- images created or shared are used to abuse peers e.g., by selling images online or obtaining images to share more widely without consent to publicly shame

Staff should avoid language that blames or shames a child and should use terminology the child is comfortable with where appropriate.

No two incidents will be identical. The school will respond consistently but proportionately, with the welfare and protection of the children involved as the primary concern. Every incident must be reported to the Designated Safeguarding Lead (DSL) or Deputy DSL as soon as possible and treated as a safeguarding concern. The DSL will consider the context, motivation, consent, age and developmental stage of the children, any vulnerabilities, the extent of sharing, and any indicators of coercion, exploitation, grooming, blackmail or adult involvement.

THE LAW

The law concerning sexual images of children exists primarily to protect children from abuse and exploitation. Taking, making, possessing, showing or distributing indecent images of a person under 18 can constitute a criminal offence, including where a child creates an image of themselves.

Relevant legislation includes the Protection of Children Act 1978 and section 160 of the Criminal Justice Act 1988. The legal concept of an indecent image includes pseudo-images, which can include computer-generated or AI-generated material that appears to be a photograph.

In particular:

- it may be an offence to take or make, possess, distribute or show an indecent image or pseudo-image of a child
- taking and sharing nude photographs of those aged under 18, including images generated using AI, is a criminal offence, and
- children should be informed about the law in a way that supports safeguarding and avoids unnecessary criminalisation or alarm. Consensual image sharing, especially between older children of the same age, may require a different safeguarding response. It may not be abusive, but children should understand that it is still illegal; non-consensual sharing is illegal and abusive.

Indecent imagery does not always mean nudity; however, images are likely to be defined as such if they meet one or more of the following criteria:

- nude or semi-nude sexual posing e.g., displaying genitals and/or breasts or overtly sexual images of young people in their underwear
- someone nude or semi-nude touching themselves in a sexual way
- any sexual activity involving a child
- someone hurting someone else sexually
- sexual activity that includes animals

Non-consensual image sharing, coercion and exploitation
Other criminal offences may also apply where intimate images are taken, created, copied, threatened or shared without consent, or where blackmail, grooming, exploitation, sexual abuse or other harmful conduct is involved. The DSL will seek advice from police and/or children's social care where required rather than attempting to determine criminal liability.

HANDLING INCIDENTS

STEP 1 – INITIAL RESPONSE

This school will manage all incidents involving the making or sharing of nudes and semi-nudes as safeguarding concerns in accordance with KCSIE 2026, the school's Safeguarding and Child Protection Policy and current UKCIS guidance.

This policy reflects the school's approach to incidents of nude and semi-nude images being shared and staff should respond to such incidents in line with it.

When an incident involving nude and semi-nude images comes to the attention of any member of staff in an education setting:

- The incident should be referred to the DSL (or equivalent) as soon as possible.
- The DSL (or equivalent) should hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns.
- There should be subsequent interviews with the children or young people involved (if appropriate).
- Parents and carers should be informed at an early stage and involved in the process in order to best support the child or young person unless there is good reason to believe that involving them would put the child or young person at risk of harm.
- A referral should be made to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process.

An initial review meeting should be held to consider the initial evidence and aim to establish the following:

- Whether there is an immediate risk to any child or young person?
- If a referral should be made to the police and/or children's social care?
- If it is necessary to view the image(s) in order to safeguard the child or young person? – in most cases, images or videos should not be viewed
- What further information is required to decide on the best response?
- Whether the image(s) has been shared widely and via what services and/or platforms? - this may be unknown
- Whether immediate action should be taken to delete or remove images or videos from devices or online services?
- What were the relevant facts about the children or young people involved which would influence risk assessment?
- If there is a need to contact another education, setting or individual?
- Whether to contact parents or carers of the children or young people involved? - in most cases they should be involved

Assessing the risks once the images have been shared

The circumstances of incidents can vary widely. If at the initial review stage, a decision has been made not to refer to police and/or children's social care, the DSL (or equivalent) should conduct a further review (including an interview with any child or young person involved) to establish the facts and assess the risks, referring back to any relevant assessment tools.

When assessing the risks and determining whether a referral is needed, the following should be also considered:

- Why was the nude or semi-nude image(s) shared? Was it consensual or was the child or young person put under pressure or coerced?
- Has the nude or semi-nude image(s) been shared beyond its intended recipient? Was it shared without the consent of the child or young person who produced the image?
- Has the nude or semi-nude image(s) been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread?
- How old are any of the children or young people involved?
- Did the child or young person send the nude or semi-nude image(s) to more than one person?
- Do you have any concerns about the child or young person's vulnerability?
- Are there additional concerns if the parents or carers are informed?
- Is there a significant age or power imbalance, or any concern about maturity, SEND, communication needs or capacity to understand or consent?
- Is there any indication of adult involvement, grooming, sexual or financial extortion (sextortion), threats, blackmail, profit motive or organised criminal activity?
- has the image been digitally altered or generated using AI, and is the child identifiable or being impersonated?

These questions will help the DSL (or equivalent) decide whether a child or young person is at risk of harm, in which case a referral will be appropriate, whether additional information or support is needed from other agencies or whether the education setting can manage the incident and support any child or young person directly. DSL(or equivalent) should always use their professional judgment in conjunction with that of their colleagues to assess incidents.

STEP 2 - SEARCHING A DEVICE – VIEWING THE IMAGERY

Any search, confiscation or examination of an electronic device must be carried out in accordance with the school's current Searching and Confiscation Policy or procedures and current DfE guidance.

Searching and Confiscation of Digital Devices

Where an electronic device is lawfully searched or confiscated, staff must first consider the safeguarding response. If a member of staff suspects that a device may contain a nude or semi-nude image of a child, they should not intentionally view the image. The device should be secured and the matter referred promptly to the DSL or Deputy DSL.

The following principles apply to devices and imagery:

- staff must follow the school's safeguarding and searching/confiscation procedures
- staff should avoid looking for or intentionally opening suspected child sexual imagery and should refer the matter to the DSL
- no member of staff should copy, print, share, store or save suspected nude or semi-nude imagery, and
- where police may need the device, it should be secured to preserve evidence and handled in accordance with police advice.

Where imagery or the surrounding circumstances indicate abuse, exploitation or another aggravating factor, the DSL will refer to police and/or children's social care through local safeguarding arrangements.

Current UKCIS and National Police Chiefs' Council guidance recognises that some lower-risk, non-abusive incidents may be managed by the school without police involvement. However, abusive or aggravating incidents should be referred to the police through the MASH or equivalent local arrangements.

A lower-risk or experimental incident is one with no adult involvement, no apparent intent to harm, no reckless misuse and no evidence of exploitation, grooming, profit motive, malicious intent or persistent behaviour. The DSL must still assess and record the incident and provide appropriate support and education.

All adult-involved incidents are child sexual abuse concerns and require immediate referral to police and children's social care through the MASH or equivalent local safeguarding route.

Where the DSL decides that police or children's social care involvement is not required, the reasons must be clearly recorded in the safeguarding record, together with the risk assessment and actions taken.

The school should avoid unnecessary examination of a child's device or imagery. Wherever possible, the DSL should establish what has happened from the child's account and other available information. If there is uncertainty about preserving evidence or whether a device should be examined, the DSL should seek police advice.

Staff and parents or carers must not intentionally view any nude and semi-nude images unless there is good and clear reason to do so as outlined below. Wherever possible, responses to incidents should be based on what DSLs (or equivalents) have been told about the content of the imagery.

It is important that all members of staff are clear on what they can and can't do in relation to viewing nude and semi-nude images and that this is communicated to any child, young person or parent and carer requesting that imagery be viewed.

The decision to view any imagery should be based on the professional judgment of the DSL (or equivalent) and should always comply with the Child protection policy and procedures of the education setting. Imagery should never be viewed if the act of viewing will cause significant distress or harm to any child or young person involved.

If a decision is made to view imagery, the DSL (or equivalent) would need to be satisfied that viewing the images:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any child or young person involved.
- Is necessary to report it to a website, app, or suitable reporting agency (such as the IWF) to have it taken down, or to support the child or young person or parent or carer in making a report.
- Is unavoidable because a child or young person has presented it directly to a staff member or nude or semi-nude images have been found on an education setting's device or network.

If it is necessary to view the imagery, then the DSL (or equivalent) should:

- Never copy, print, share, store or save them; this is illegal. If this has already happened, please contact your local police for advice and to explain the circumstances.
- Discuss the decision with the Headteacher/Principal or a member of the senior leadership team.
- Make sure viewing is undertaken by the DSL (or equivalent) or another member of the safeguarding team with delegated authority from the Headteacher/Principal or a member of the senior leadership team.
- Make sure viewing takes place with another member of staff present in the room, ideally the Headteacher/Principal or a member of the senior leadership team. This staff member does not need to view the images.
- Wherever possible, make sure viewing takes place on the premises of the education setting, ideally in the Headteacher/Principal or a member of the senior leadership team's office.
- Make sure wherever possible that the images are viewed by a staff member of the same sex as the child or young person in the images.
- Record how and why the decision was made to view the imagery in the safeguarding or child protection records, including who was present, why the nude or semi-nude images were viewed and any subsequent actions. Ensure this is signed and dated and meets any appropriate wider standards e.g., such as those set out in statutory safeguarding guidance and local authority policies and procedures.
- If any devices need to be taken and passed onto the police, confiscate the device(s), and call the police. The device should be disconnected from Wi-Fi and data and turned off immediately to avoid imagery being removed from the device remotely through a cloud storage service. The device should be placed in a secure place, for example in a locked cupboard or safe until the police are able to come and collect it.

Informing parents and carers

Parents or carers should be informed and involved in the process at an early stage unless informing them will put a child or young person at risk of harm. Any decision not to inform the parents or carers should be made in conjunction with other services such as children's social care and/or the police, who would take the lead in deciding when they should be informed.

Where appropriate, DSL (or equivalents) should support any child or young person involved with determining the best approach for informing parents and carers and allow them to be a part of this process if they want to be.

If there is an indecent image of a child on a website or a social networking site, then the Safeguarding Team will report the image to the site hosting it. Under normal circumstances the team would follow the reporting procedures on the respective website; however, in the case of a sexual imaging incident involving a child or young person where it may be felt that they may be at risk of abuse then the team will report the incident directly to CEOP:Report to CEOP so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Once the DSL has enough information, the decision should be made whether to deal with the matter in school or refer it to the police/social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt with in school, a further review should be held to assess risks.

The DSL should refer to police and/or children's social care, as appropriate, where the incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent, [e.g., SEND]
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm because of the disclosure (for example, self-harm or suicide)

STEP 3 - WHAT TO DO AND NOT DO WITH THE IMAGE

<u>If the image has been shared across a personal mobile device:</u>

Always
Confiscate and secure the device(s).
Close down or switch the device off as soon as possible. This may prevent anyone removing evidence 'remotely'.

Never
Intentionally view the image unless the DSL has determined, in exceptional circumstances, that viewing is necessary to safeguard a child and the viewing is carried out in accordance with this policy.
Send, share, or save the image anywhere (this is illegal).
Ask or allow children to view, copy, share, store or save the imagery.

<u>If the image has been shared across a school network, a website, or a social network:</u>

Always
Contact the school's authorised IT lead promptly so that access to the material can be restricted or contained without unnecessarily viewing, copying or circulating it, while preserving any evidence that may be required by police.

Never
Send or print the image
Move, download or transfer the material unless specifically advised to do so by police or another appropriate authority.
View the image outside of the protocols in the school's safeguarding and child protection policies and procedures.

<u>Deleting images (from devices and social media)</u>

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting nude and semi-nude images from devices and online services to limit any further sharing.

In most cases, children and young people should be asked to delete the imagery and to confirm that they have deleted them. They should be given a deadline for deletion across all devices, online storage, or social media sites. They should be reminded that possession of nude and semi-nude images is illegal. They should be informed that if they refuse or it is later discovered they did not delete the imagery, they are continuing to commit a criminal offence, and the police may become involved.

Any decision to search a child or young person's device and delete imagery should be based on the professional judgment of the DSL (or equivalent) and should always comply with the safeguarding or child protection policy and procedures of the education setting. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding

records. Parents and carers should also be informed unless this presents a further risk to any child or the young person.

STEP 4 – RECORDING INCIDENTS

All incidents relating to nude and semi-nude images being shared need to be recorded. This includes incidents that have been referred to external agencies and those that have not. Incidents that have not been reported to police or children's social care by education settings should record their reason for doing so and ensure it is signed off by the Headteacher. Please note copies of imagery should not be taken.

Records should be kept in line with statutory requirements set out in Keeping Children Safe in Education, where applicable, and the local safeguarding procedures.

STEP 5 - DECIDING ON A RESPONSE

There may be many reasons why a child has made or shared a nude or semi-nude. The response must distinguish, so far as possible, between lower-risk consensual or exploratory behaviour and incidents involving coercion, abuse, exploitation, malicious sharing, grooming, adult involvement or financial extortion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident (see Supplement 1 for definitions). However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If nudes or semi-nudes of a child are identified or reported:

- Act in accordance with the Safeguarding Policy i.e. inform the Safeguarding Team.
- Store the device securely.
- The Safeguarding Team should carry out a risk assessment in relation to the young person (Use Appendices 2 and 3 for support).
- The Safeguarding Team will make a referral if needed.
- The DSL will decide, using current UKCIS guidance and local safeguarding procedures, whether police and/or children's social care should be involved. Adult-involved incidents and incidents with abusive or aggravating factors must be referred. Lower-risk incidents may be managed within school where this is judged safe and proportionate, with the decision and rationale recorded.
- The school will put appropriate safeguards and support in place for every child involved. This may include pastoral support, counselling, online-safety support, safety planning, reasonable adjustments and action to prevent bullying, retaliation or further sharing.
- Inform parents and/or carers about the incident and how it is being managed.

Reporting nude and semi-nude images online

Children and young people may need help and support with the removal of nude and semi-nude images from devices and social media, especially if they are distressed. Most online service providers offer a reporting function for account holders, and some offer a public reporting function to enable a third party to make a report on behalf of the child or young person. More information can be found on individual providers' websites where they should make public their Terms of Service and process for reporting.
In the event that a site has no reporting function and if the content is a sexual image of someone under 18, you can report it to the Internet Watch Foundation (IWF). You can report directly to the IWF here: Internet Watch Foundation

Children and young people can use the IWF and Childline's Report Remove tool to report images and videos they are worried have been, or might be, shared publicly at Online safety | Childline

The tool helps children and young people to report an image shared online, to see if it is possible to get the image removed. This must be done as soon as possible in order to minimise the number of people that have seen the picture.
If you are concerned that a child or young person is being sexually abused, exploited, or groomed online you should report to NCA-CEOP: CEOP

Supporting parents and carers
For advice on supporting parents and carers see the UKCIS document 'Sharing nudes and semi-nudes'

STEP 6 - CONTAINMENT AND PREVENTION

Children involved in an incident may remain distressed or vulnerable after the immediate issue has been contained. Appropriate pastoral and safeguarding support will therefore continue for as long as needed, including consideration of self-harm, suicide risk, bullying, exploitation and ongoing online contact. Where incidents indicate a wider pattern or unsafe culture, the school will reinforce age-appropriate education about consent, respectful relationships, online safety, image sharing, AI-generated imagery, deepfakes, sexual coercion and how to seek help.

Other staff may need to be informed of incidents and should be prepared to act if the issue is continued or referred to by other pupils. The school, its pupils and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected.

The pupils' parents should usually be told what has happened so that they can keep a watchful eye over the young person especially when they are online at home.

STEP 7 - REVIEW OUTCOMES AND PROCEDURES WITH THE AIM OF PREVENTING FUTURE INCIDENTS

The frequency or severity of such incidents may be such that the school will need to review its approach.

Where this is the case, this school will do the following:

- Ensure that key policies e.g. Safeguarding, Anti- Bullying, Authorised User Policies are still relevant and can meet emerging issues.
- Ensure that the school's infrastructure and technologies are robust enough to meet new challenges.
- Ensure that both adults and young persons are alerted to the issues such as safety mechanisms, support mechanisms and the legal implications of such behaviour.
- Review relevant safeguarding, behaviour, RSHE and online-safety arrangements and take account of current statutory and non-statutory guidance.

Incidents may arise on personal or school devices, online or offline, and may involve genuine, altered or AI-generated imagery. The school will provide preventative education and appropriate staff training so that concerns are recognised and managed consistently.

Useful current sources include:
NCA-CEOP Education resources and the CEOP Safety Centre
Childnet and UK Safer Internet Centre resources on online sexual harassment, consent and image sharing
The IWF/Childline Report Remove service and, where appropriate,
NCMEC Take It Down alongside current UKCIS guidance on reporting and removal of imagery.

SHARING NUDES AND SEMI-NUDES - SUPPLEMENT 1

THE LEGAL POSITION AND POLICE RESPONSE

The Protection of Children Act 1978 and section 160 of the Criminal Justice Act 1988 criminalise specified conduct involving indecent photographs and pseudo-images of children under 18. Pseudo-images can include digitally created or AI-generated material that appears to be a photograph.

Depending on the circumstances, offences may include:

- taking an indecent photograph or allowing an indecent photograph to be taken
- making an indecent photograph (this includes downloading or opening an image that has been sent via email)
- distributing or showing such an image
- possessing with the intention of distributing images
- advertising, and
- possessing such images.

Any decision about crime recording, investigation, charge or prosecution is a matter for the police and Crown Prosecution Service.

The safeguarding response should avoid unnecessarily criminalising children. Police involvement does not automatically result in a criminal record or formal sanction. Current police practice allows proportionate outcomes in non-abusive cases, including Outcome 21 where appropriate.

Where an incident is non-abusive and there is no evidence of exploitation, grooming, profit motive, malicious intent or persistent behaviour, police may decide that further formal action is not in the public interest. Where there are abusive or aggravating factors, the matter should always be referred to police through the MASH or equivalent.

The school's role is to safeguard, assess risk, record its decisions and refer where required. It is not the school's role to decide whether a criminal offence should be charged or prosecuted.

Children should be helped to understand the legal position in an age-appropriate way, while making clear that the purpose of the response is to protect and support them, not to shame or automatically criminalise them.

SHARING NUDES AND SEMI-NUDES - SUPPLEMENT 2

ASSESSING DIFFERENT TYPES OF INCIDENT

Current UKCIS guidance continues to use Finkelhor and Wolak's typology as one tool for distinguishing aggravated incidents from experimental incidents. It should be used alongside professional judgment and the full 2024 UKCIS guidance.

Aggravated incidents involving criminal or abusive elements beyond the creation, sending or possession of youth-produced sexual images

Adult-involved: an adult, criminal group or person posing as a child may groom, coerce or exploit a child to obtain imagery. This includes sexually motivated abuse and financially motivated sexual extortion (sextortion). Adults may use stolen, digitally manipulated or AI-generated images to blackmail a child. All adult-involved incidents are child sexual abuse and require immediate referral to police and children's social care through local arrangements.

Youth Only – Intent to Harm: incidents that may:

- arise from interpersonal conflict such as break-ups and fights among friends
- involve criminal or abusive conduct such as blackmail, threats, or deception
- involve criminal sexual abuse or exploitation by juvenile offenders.

Youth Only – Reckless Misuse: incidents where imagery is taken, created, altered or shared without the knowing or willing participation of the child pictured, including reckless forwarding or AI manipulation. A child may be harmed even where there was no specific intent to harm.

Experimental incidents: involve the creation or sharing of nudes and semi-nudes with no adult involvement, no apparent intent to harm and no reckless misuse. They still require safeguarding assessment, recording, support and appropriate education.

Romantic episodes: in which young people in ongoing relationships make images for themselves or each other, and images were not intended to be distributed beyond the pair.

Sexual Attention Seeking: in which images are made and sent between or among young people who were not known to be romantic partners, or where one youngster takes pictures and sends them to many others or posts them online, presumably to draw sexual attention.

Other: cases that do not appear to have aggravating elements, like adult involvement, malicious motives, or reckless misuse, but also do not fit into the Romantic or Attention Seeking sub-types. These involve either young people who take pictures of themselves for themselves (no evidence of any sending or sharing or intent to do so) or pre-adolescent children (age 9 or younger) who did not appear to have sexual motives.

HOW TO RESPOND TO AN INCIDENT – SUPPLEMENT 3

An overview for all staff working in education settings in England

This document provides a brief overview for frontline staff of how to respond to incidents where nude and semi-nude images have been shared.

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with the school's child protection policies.

The DSL or Deputy DSL should use the full UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people, updated March 2024, together with KCSIE 2026. This short supplement does not replace the full guidance.

What do we mean by sharing nude and semi-nude images?
Current guidance defines making or sharing nudes and semi-nudes as the creation, sending or posting of nude or semi-nude images by young people under 18. Images include photographs, videos and livestreams and can be shared online or directly between devices. They may be genuine, digitally altered or wholly generated using AI, including deepfakes or deep nudes.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

Where an adult is involved in obtaining, creating or sharing nudes or semi-nudes of a child, this is a child sexual abuse concern and must be referred immediately to police and children's social care through the MASH or equivalent local safeguarding route.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately.

The school's Child Protection Policy code of practice to be followed is as follows:

- Never intentionally view, copy, print, share, store or save the imagery yourself, or ask a child to share or download it. In exceptional circumstances the DSL may decide that viewing is necessary to safeguard a child; this must be based on professional judgment and recorded.
- If you have already viewed the imagery accidentally, report this to the DSL or Deputy DSL immediately and seek support if needed.
- Do not delete the imagery or ask the child to delete it at the initial reporting stage. The DSL will decide what action is appropriate after the initial review and any necessary police or social care advice.
- Do not question the child in detail about the imagery. Listen, reassure, record what has been said and leave further information-gathering to the DSL or Deputy DSL.
- Do not share information about the incident beyond those who need to know. Parents and carers will normally be informed at an early stage by or in consultation with the DSL, unless this would place a child at risk of harm.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Remember: report immediately to the DSL or Deputy DSL; do not blame or shame; do not circulate imagery; and reassure the child that they will be supported.