Denefield School

Data protection, e-safety and acceptable use policy

Approved by Resources on	18 March 2026
Date of next review	March 2027
Review cycle	Annual
Policy control sheet updated	Yes
Type of policy	Statutory
Policy owner	Director of Operations (HML)
Location of policy	Website

Denefield School

Data protection, e-safety and acceptable use policy

Contents

1. Introduction and aims

ICT is integral to Denefield School's teaching, learning, pastoral and operational activity. These technologies bring considerable benefits but also introduce risks to data protection, online safety and safeguarding. This policy sets out how the school manages those risks and the standards of acceptable use expected of everyone who uses our ICT facilities.

This policy applies to all users of school ICT facilities and services, including trustees, staff, students, volunteers, contractors and visitors. It also covers the use of school-provided devices off-site and the limited personal use of ICT facilities by staff where permitted.

- **We aim to:**
  - Ensure all personal data about staff, students, parents/carers, trustees, volunteers and visitors is collected, used, shared and retained lawfully, fairly and securely under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- **E-safety aims**:
  - Deliver a whole-school approach that protects and educates the school community in its use of technology, with clear mechanisms to identify, report, intervene and escalate concerns.
- **Acceptable use aims:**
  - Set clear, proportionate rules for using the school's ICT systems and internet, including what constitutes unacceptable use and the potential sanctions for misuse.
- **Safeguarding aims:**
  - Support statutory safeguarding guidance, including Keeping Children Safe in Education (KCSIE), and align with related policies (child protection, behaviour, staff discipline).

2. Legislation and guidance

This policy reflects requirements under the UK GDPR and the DPA 2018, as interpreted and explained by the Information Commissioner's Office (ICO). It also draws on sector guidance and relevant education law.

Key legislation and guidance includes:

- UK GDPR and Data Protection Act 2018 (including principles, individual rights, lawful bases, special category and criminal offence data, security, accountability).
- Protection of Freedoms Act 2012 (biometric information of children in schools and colleges).
- ICO guidance on CCTV and video surveillance, security and personal data breaches.
- Department for Education (DfE) statutory guidance: Keeping Children Safe in Education (current edition) and non-statutory guidance: Teaching online safety in schools.
- DfE guidance: Searching, screening and confiscation (for the examination of electronic devices).
- Other relevant law: Human Rights Act 1998, Equality Act 2010, Computer Misuse Act 1990, Freedom of Information Act 2000, Education Acts and relevant regulations.

3. Definitions

Personal data: Any information relating to an identified or identifiable living individual (for example, name, identification numbers, location data, online identifiers, or factors specific to identity).

Special category personal data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data for identification, health data, or data concerning sex life or sexual orientation.

Processing: Any operation performed on personal data, whether automated or not (such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, erasure or destruction).

Data subject: The identified or identifiable individual whose personal data is processed.

Data controller: The organisation that determines the purposes and means of the processing of personal data (Denefield School).

Data processor: A person or organisation (other than the controller's employees) that processes personal data on behalf of the controller.

Personal data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ICT facilities: The school's ICT network, services, systems, hardware and software (including cloud services), whether used on-site or remotely, on school or authorised personal devices.

Users: Anyone authorised by the school to use the ICT facilities, including trustees, staff, students, volunteers, contractors and visitors.

Personal use: Any use not directly related to a user's employment, study or official purpose.

Authorised personnel: Employees or contractors authorised by the school to administer and/or monitor the ICT facilities.

Materials: Files and data created or stored using ICT facilities (documents, photos, audio, video, web pages, social networking, blogs, etc.).

4. Denefield as the data controller

Denefield School is the data controller for the personal data it processes about students, parents/carers, staff, trustees, volunteers and visitors. The school is registered with the ICO as required by law.

5. Roles and responsibilities

This policy applies to all staff employed by the school and to external organisations or individuals working on our behalf. Staff who do not comply may face disciplinary action. Relevant parts also apply to trustees, volunteers, parents/carers, students and visitors.

5.1 Trust board: Has overall responsibility for ensuring compliance with data protection obligations, monitoring this policy and holding the headteacher to account. The board coordinates regular discussions on online safety and reviews logs provided by the designated safeguarding lead (DSL).

5.2 Data protection officer (DPO): Oversees implementation of this policy; monitors compliance; advises on data protection obligations; is the contact point for data subjects and the ICO; and reports annually to the Trust Board. DPO: Paul Hamilton (HML@denefield.org.uk).

5.3 Headteacher: Acts as the representative of the controller on a day-to-day basis and ensures consistent implementation of this policy across the school.

5.4 All staff (including contractors, agency staff and volunteers): Must understand and apply this policy; handle personal data lawfully and securely; follow acceptable use rules; and work with the DSL to ensure online safety incidents are logged and addressed.

5.5 Designated safeguarding lead (DSL): Leads on online safety; ensures incidents are logged and addressed; updates and delivers staff training; liaises with external agencies; and provides regular reports to the headteacher and/or Trust Board.

5.6 Director of Operations: Ensures appropriate filtering and monitoring; maintains ICT security (including updates, anti-malware, firewalls); conducts regular checks; blocks dangerous content; logs online safety incidents; and ensures cyber-bullying incidents are addressed in line with the behaviour policy.

5.7 Parents/carers: Should raise queries or concerns about this policy and ensure their child understands and signs the student acceptable use agreement (appendix).

5.8 Students: Must read, understand and sign the acceptable use agreement and follow the rules at all times.

5.9 Visitors and members of the community: Where relevant, will be made aware of this policy and are expected to follow it. Where appropriate, visitors will sign an acceptable use agreement.

6. Data protection principles

The school adheres to the data protection principles set out in the UK GDPR. Personal data must be:

- Processed lawfully, fairly and transparently;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;

- Kept for no longer than is necessary; and
- Processed in a manner that ensures appropriate security (confidentiality, integrity and availability).
- Accountability: the school is responsible for, and must be able to demonstrate, compliance with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency: We process personal data only where a lawful basis applies (contract, legal obligation, vital interests, public task, legitimate interests, or consent). For special category data we also meet a condition in Article 9 UK GDPR or the DPA 2018 (for example, employment law, vital interests, substantial public interest, health or social care, public health, or research). For criminal offence data we meet a lawful basis and an appropriate condition in the DPA 2018.

We provide data subjects with the information required by data protection law when we first collect personal data (via privacy notices) and we will not use personal data in ways that are unfair or unexpected.

7.2 Limitation, minimisation and accuracy: We collect personal data for specified, explicit and legitimate purposes, and will not use it for incompatible purposes without informing individuals and, where necessary, obtaining consent. Staff will only process the personal data they need to carry out their roles. We keep data accurate and up to date and rectify or erase inaccurate data when appropriate. When personal data is no longer needed, we delete or anonymise it in line with our retention schedule.

8. Sharing personal data

We do not normally share personal data without consent. We may share data where necessary, for example: to protect staff or students; to liaise with other agencies; with suppliers or contractors to deliver services (under a compliant contract); with law enforcement or government bodies where legally required; or with emergency services and local authorities in response to incidents.

Where we use processors, we only appoint suppliers providing sufficient guarantees of compliance and put in place data protection contracts. We only share the minimum data necessary for the task.

International transfers: Where we transfer personal data outside the UK, we will comply with UK data protection law (for example, using adequacy regulations, International Data Transfer Agreements, or UK Addenda to Standard Contractual Clauses).

9. Subject access requests and other rights

9.1 Subject access requests (SARs): Individuals have the right to obtain confirmation that we process their personal data and access to a copy of that data, together with supplementary information. Requests may be made in any form; written requests are helpful where possible. Staff must forward any SAR to the DPO immediately.

We may ask for reasonable identification, may telephone to confirm a request, and will respond without undue delay and within one month of receipt (or from receiving ID where relevant). Where requests are complex or numerous, we may extend by up to two further months and will explain why within one month. We will normally provide information free of charge.

We may withhold information in limited circumstances (for example, where disclosure would cause serious harm to the physical or mental health of any individual, would reveal safeguarding information contrary to the child's best interests, would disclose another person's personal data that cannot reasonably be anonymised, or is legally privileged). Where a request is unfounded or excessive, we may refuse or charge a reasonable fee.

9.2 Children and SARs: Personal data about a child belongs to that child. Competence depends on the child's ability to understand their rights; a general presumption is that many children aged 12 or over will be competent, but this will be assessed case by case. Where a parent/carer makes a SAR on behalf of a child who is competent, we will usually need the child's consent.

9.3 Other rights: Individuals may ask us to rectify inaccurate data; erase data; restrict processing; object to certain processing (including public task or legitimate interests); and exercise rights in relation to automated decision-making/profiling. Individuals may also make complaints to the ICO and, in certain circumstances, request data portability.

10. Parental requests to see the educational record

As an academy, Denefield School is not legally obliged to provide access to a pupil's educational record under The Education (Pupil Information) (England) Regulations 2005, which apply to maintained schools and certain special schools. Parents/carers may still request personal data under data protection law (for example, via a subject access request). Where available, copies of reports can be requested from the school in line with our usual processes.

11. Biometric recognition systems

The school complies with the Protection of Freedoms Act 2012 and DfE guidance when using biometric systems. Processing biometric data requires parental consent for students under 18; if the student or any parent objects, processing must stop. Alternative arrangements (e.g., PIN) are always offered.

12. CCTV

CCTV is used for site safety in accordance with ICO video surveillance guidance. Cameras operate overtly with signage. Footage is securely stored, access-controlled, and retained only as long as necessary.

13. Photographs and videos

Parents/students over 18 provide consent for use of images. The school explains how images will be used in our privacy notice and avoids publishing identifying information. Consent may be withdrawn at any time.

14. Data protection by design and default

The school embeds data protection into systems and processes through DPIAs, minimisation, secure-by-design procurement, and staff training. Records of processing and privacy notices are kept current.

15. Data security and storage of records

Paper and electronic records are protected by physical and technical controls. Devices are encrypted; passwords must be strong; staff must not reuse personal passwords. Personal data on personal devices must follow equivalent protection.

16. Disposal of records

Personal data is securely deleted or shredded when no longer required, following the retention schedule. Third-party disposal services must offer GDPR-compliant assurances.

17. Personal data breaches

All staff must report suspected breaches immediately to the DPO. The school assesses risks, mitigates impact, documents the breach and, where required, reports to the ICO within 72 hours.

18. Use of AI in school

AI may be used to enhance teaching, learning, planning and efficiency, provided its use is safe, transparent, ethical and compliant with DfE guidance.

18.1 Acceptable AI Use: Staff may use AI for lesson preparation, resource creation, administrative tasks and personalised learning support where appropriate. Students may use AI for learning support where permitted by teachers.

18.2 Prohibited AI Use: AI must not be used to generate misleading content, complete assessed work, create or share harmful or inappropriate material, or process personal data without authorisation.

18.3 Safeguarding and Data Protection: AI tools must not be used to input identifiable personal data unless the system has been approved by the school. Staff must assess risks and ensure compliance with UK GDPR and DPA 2018.

18.4 Academic Integrity: AI must never replace a student's own work in assessments or NEA. Students must declare any AI use as required by teachers and / or exam boards.

18.5 Monitoring and Compliance: The school may monitor AI usage and take action where policies are breached. Staff must report any AI-related concerns or incidents to the DSL or DPO.

19. Educating students about online safety

Online safety is taught across the curriculum and assemblies. Students learn safe, respectful use of technology, recognising risks, reporting concerns and understanding privacy.

20. Educating parents about online safety

Parents receive guidance through letters, website content and events. The school signposts national online-safety resources and encourages safe home practices.

21. Cyber-bullying

Cyber-bullying is treated as a safeguarding and behavioural concern. Staff respond promptly, support students affected and may involve external agencies. Searching devices follows DfE guidance on searching, screening and confiscation.

22. Acceptable use

All users must use school ICT systems responsibly, lawfully and in line with safeguarding and data-protection requirements. Acceptable use agreements apply to staff, students, trustees, volunteers and visitors.

23. Students using mobile devices in school

Students may bring mobile devices at their own risk but may not use them on school grounds. Breaches of the acceptable use agreement may lead to confiscation and sanctions.

24. Staff using work devices outside school

Staff must not install unauthorised software. Devices must be encrypted, password-protected and used only for work purposes. Concerns about security must be reported to ICT support immediately.

25. Unacceptable use

Unacceptable uses include but is not limited to: accessing illegal or inappropriate content, breaching copyright, sharing confidential information, enabling unauthorised access, damaging ICT systems, bypassing filters or using offensive language.

26. How the school will respond to issues of misuse

Misuse is addressed proportionately under the behaviour or staff-disciplinary policy. Serious incidents may be referred to external agencies including the police.

27. Data security

26.1 Passwords: Passwords must be strong, unique and not shared. Users are responsible for securing their accounts.

26.2 Software updates: All devices must allow automatic updates and anti-virus protection.

26.4 Access controls: Users may only access systems they are authorised to use and must log out when leaving devices unattended.

26.5 Encryption: Portable devices and removable media must be encrypted.

26.6 Servers and cloud services: All servers must be secured, patched and access-restricted; cloud providers must meet UK GDPR requirements.

28. WiFi access

School WiFi is secured. Passwords are not shared. Devices requiring access must be configured by ICT technicians. Filtering applies to all users.

29. Training

All staff receive data-protection and online-safety training on induction and annually thereafter. Trustees and volunteers receive appropriate training. DSL training occurs at least every 2 years with annual refreshers.

30. Monitoring arrangements

The DPO reviews this policy every 2 years. The DSL logs safeguarding and online-safety incidents; these are monitored regularly.

31. Links with other policies

This policy links to the school's Freedom of Information publication scheme, safeguarding policy, behaviour policy, data protection policies, complaints procedure and staff disciplinary procedures.

Appendix 1: Personal data breach procedure

This procedure is based on "guidance on personal data breaches" produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people
- The DPO will alert the headteacher and the chair of trustees for a serious breech
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will determine if the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the school DPO.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:
    - other categories and approximate number of individuals concerned
    - the categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

Appendix 2: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	
I will read and follow the rules in the acceptable use agreement policy When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only, in line with the school Data protection, e-safety and acceptable use policy • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it I will not: • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: • I will not use it within the school grounds I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (student):	Date:
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Appendix 3: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS	
Name of staff member/trustee/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students without checking with teachers first • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Director of Operations know, if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/trustee/volunteer/visitor):	Date:

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5: Social Media cheat sheet for staff

Don't accept friend requests from students on social media

10 rules for school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling social media apps from your phone. The apps recognise Wi-Fi connections and make friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students)

Check your privacy settings

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your old posts and photos – search on a search engine, such as Google, to find out how to limit the visibility of previous posts

The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't search for you by name – search on a search engine, such as Google, to find out how to do this

Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A student adds you on social media

In the first instance, ignore and delete the request. Block the student from viewing your profile Check your privacy settings again, and consider changing your display name or profile picture

If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to the relevant social network and ask them to remove it

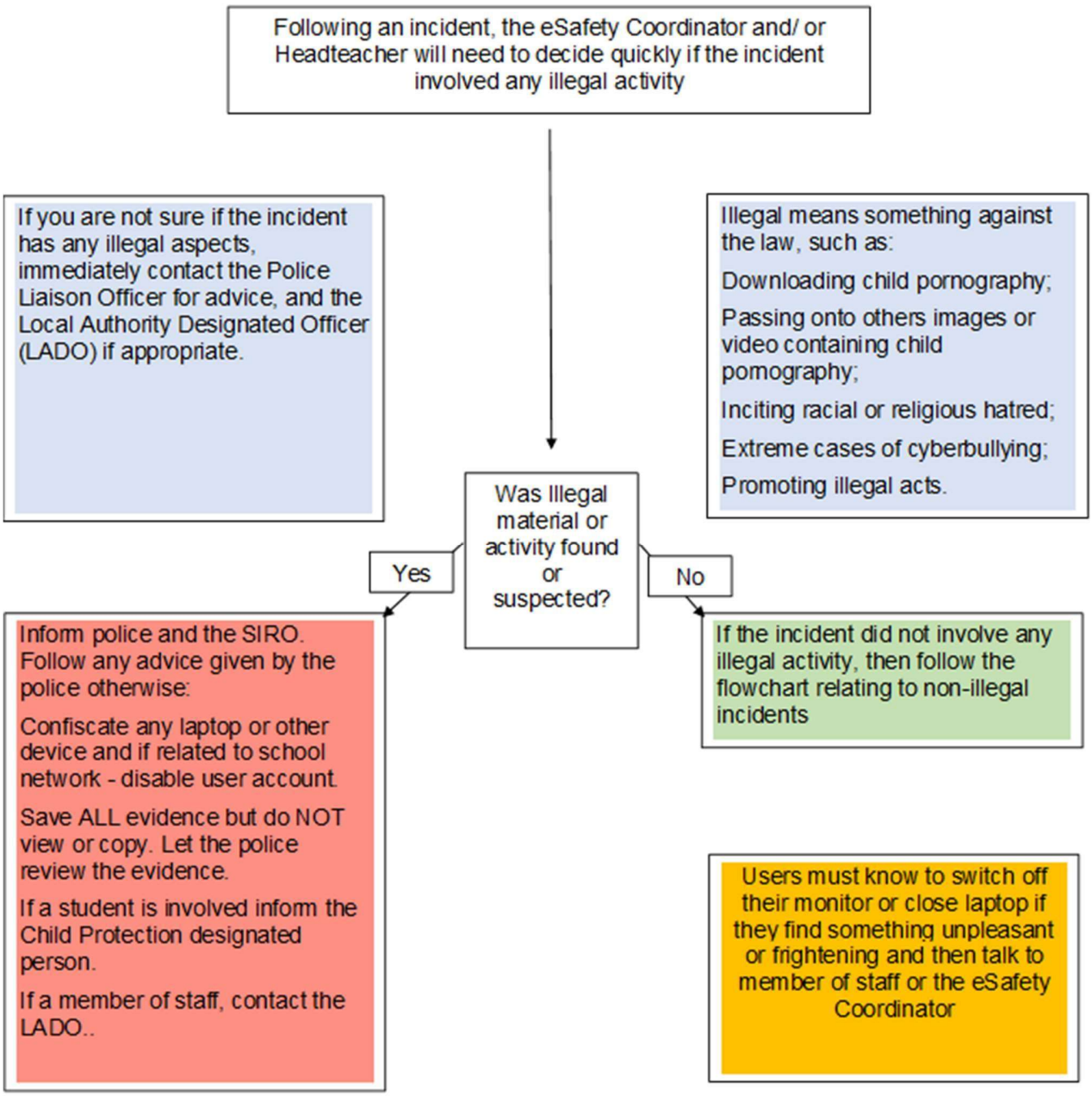
If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 6: Flowcharts for managing eSafety incidents

Flowchart to support decisions related to an illegal eSafety incident



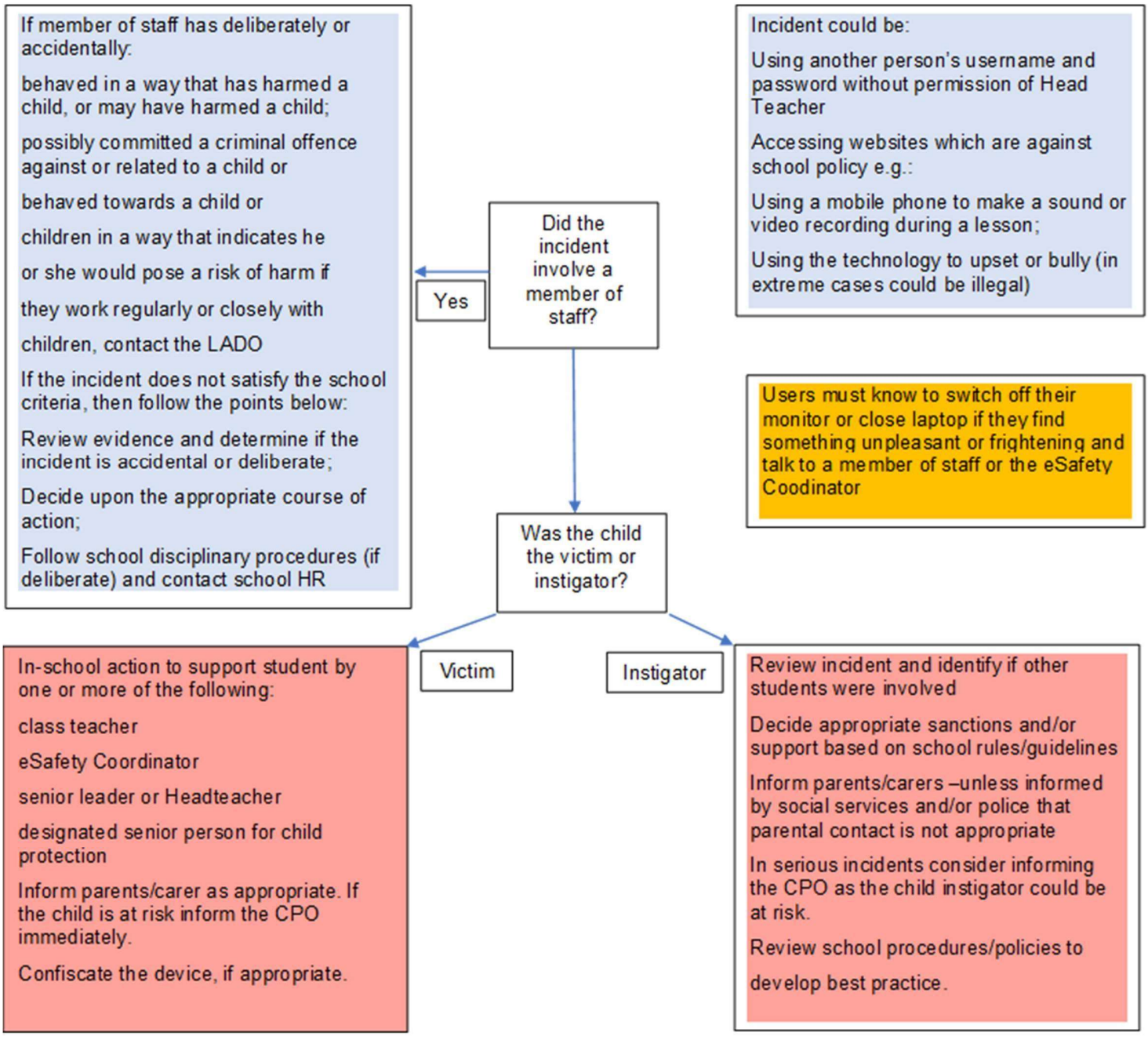
Flowchart to support decisions relating to other eSafety incidents

If the incident **did not** involve **any illegal activity,** then follow this flowchart

The eSafety coordinator and/or Headteacher should:

Record in the school eSafety Incident Log

Keep any evidence



Flowchart for managing an eSafety incident involving staff as victims

All incidents should be reported to the Headteacher, Designated safeguarding officer or Trustees who will:

Record in the school eSafety Incident Log;

Keep a written form of evidence for incidents and where the incident is related to images/screen shots describe the evidence in words and record website address without accessing or saving the images in question

Use the 'Report Abuse' button if appropriate or available

Reporting the incident to the Trustees.

Parents/carers as instigators - follow some of the steps below:

Contact the person and invite into school and discuss using some of the examples below:

You have become aware of discussions taking place online;

You want to discuss this

You have an open-door policy so disappointed they did not approach you first;

They have signed the Home School agreement;

Request the offending material be removed

If this does not solve the problem, consider involving the Chair of Trustees.

Staff as instigators - follow some of the steps below:

Contact School HR for initial advice and/or contact the eSafety coordinator;

Contact the member so staff and request the offending material be removed immediately, in serious cases you may be advised not to discuss the incident with the staff member;

Refer to the signed ICT Acceptable Use Agreement and consider if this incident has an impact on the Contract of Employment of the member of staff..

Students as instigators - follow some of the steps below:

Identify the students involved;

Ask student to remove offensive material. Refer to signed Acceptable Use Agreement.

If the perpetrator refused to remove the material and is under 13, contact the Social Network who will close the account.

Take appropriate actions in-line with school policies/rules.

Inform parents/carers unless informed by social services and/or police that parental contact is not appropriate

if the child is at risk talk to your school Child Protection designated person

Further contacts to support staff include:

School eSafety adviser

School HR

School Governance

Local Police

LA legal team helpline

The Headteacher or Chair of Trustees can be the single point of contact to coordinate responses.

The members of staff may also wish to take advice from their union.

For serious incidents or further advice:

Inform your local police neighbourhood team;