



Responding to Complaints, Bullying and Harassment on Social Media

Guidance for Education Setting Leaders
and Designated Safeguarding Leads

Contents

1. Introduction	4
Relationship with National Guidance	5
2. Responding to concerns raised on social media	6
Distinguishing criticism, bullying and harassment.....	6
Respond calmly and proportionately.....	7
Preserve and record relevant information.....	7
Identify who will lead the response	8
Record keeping	9
Supporting those affected	10
Supporting staff	10
Supporting other members of the community.....	12
Discriminatory bullying and harassment.....	13
Meet with the parent or carer where safe and appropriate	13
3. Where concerns remain unresolved or require further action.....	16
Arrange a further meeting.....	16
Report content to the platform	17
Seek further advice.....	17
Legal and employment advice.....	17
Allegations concerning a person working with children	18
Police advice	18
Safeguarding children/learners.....	18
Safeguarding adults.....	19
Media interest.....	19
Concerns raised by members of the public.....	19
Concerns raised by children/learners	20
Concerns raised by staff	21
4. Preventative Action.....	22
Employer and governance oversight	22
Build a whole community approach to positive online behaviour.....	23
Supporting staff to manage their online safety.....	24
Acceptable Use of Technology Policies (AUP).....	25
Setting policies and procedures.....	26

Supporting staff to raise concerns	27
Parental codes of conduct and shared expectations	27
Promote positive use of social media	28
Provide accessible routes for raising concerns.....	29
5. Responding to Fake, Anonymous and Misleading Accounts, including AI-generated content.....	30
Understanding AI-generated or manipulated content.....	30
Responding to concerns	31
Preserve relevant information	32
Undertake proportionate internal enquiries	33
Responses where the person responsible has been identified	34
Supporting affected staff and children/learners.....	35
Report and escalate concerns	36
Preventative action	37
6. Conclusion.....	38
Appendix One: Responding to Concerns Flowchart	39
Appendix Two: Legal Information	40
Criminal concerns	40
Civil concerns: defamation, privacy and confidentiality	42
Appendix Three: Template letters	43
Preventative approaches	43
General Awareness Information for Newsletters	43
General Awareness Letter for all parents	43
Letters following specific issues.....	46
Template incident letter for use with all parents/carers.....	46
Letter to use with parents specifically involved in concerns.....	47
Disclaimer and Copyright	49

This document was last updated August 2026

1. Introduction

Social media can provide education settings with valuable opportunities to communicate with parents and carers, share information, celebrate achievements and engage with their wider communities. However, concerns, complaints and comments about a setting or members of its community may also be shared online, where they can spread quickly and reach a wide audience.

Everyone is entitled to express an opinion or raise a legitimate concern. Negative comments, criticism or disagreement should not automatically be characterised as bullying or harassment. Where possible, concerns about an education setting should be raised through its established communication or complaints procedures so that they can be properly understood and addressed.

In some circumstances, online content may identify, target or cause harm to a child/learner, family, member of staff or other person connected with the setting. It may include bullying, harassment, discrimination, threats, allegations, impersonation, misleading information or manipulated content. Such content can affect the safety and wellbeing of individuals and the wider setting community. It may also raise safeguarding, staff conduct, health and safety, employment or potentially criminal concerns.

There is no single response that will be appropriate in every situation. Settings should consider the nature, context and impact of the content, any pattern of behaviour, the needs and views of those affected, and whether immediate safeguarding or safety action is required. Responses should be fair, proportionate and consistent with the setting's relevant policies and procedures.

Settings should take a proportionate approach to monitoring or searching for online content. Routine surveillance of parents, carers, children/learners or staff is unlikely to be appropriate. However, where a concern has been reported, an appropriately authorised leader may need to locate, preserve or report relevant content. Any enquiries should be necessary, proportionate and limited to information lawfully available to the setting.

The potential impact on the person reviewing harmful or distressing material should also be considered, and appropriate support provided. Staff may choose to review their own public online presence and privacy and security settings as part of protecting their personal safety and professional reputation.

Education is a public matter, so it is important to understand that a level of scrutiny is inevitable at times. Online censorship will not be possible, so a proportionate and measured response should be taken by leaders where content impacts on the daily running of a setting or poses a risk of harm to members of the community.

Relationship with National Guidance

This guidance has been developed by [Kent County Council's LADO Education Safeguarding Advisory Service](#) (LESAS) to support education settings in responding to complaints, bullying, harassment and other concerns shared through social media.

Schools and colleges should read this guidance alongside the version of [Keeping children safe in education](#) (KCSIE) currently in force. Early years providers should follow the safeguarding requirements of the [Early Years Foundation Stage](#) (EYFS) framework and any other requirements applying to their provision.

This document should also be read alongside the Department for Education's (DfE) non-statutory guidance, [Preventing and tackling bullying and harassment of school staff](#). This guidance applies directly to maintained schools, academies and their employers. Other education providers may find its principles helpful, but should note that some legal duties, governance arrangements and procedures may differ.

For the purposes of the DfE's [staff bullying and harassment guidance](#), "school staff" refers to employees and agency workers and does not include volunteers. Settings should nevertheless consider their safeguarding, safety and support responsibilities towards volunteers under the arrangements applicable to them.

Where online comments amount, or may amount, to bullying, harassment, discrimination, intimidation or threats against a member of staff, the matter should not be treated solely as a complaint or reputational issue. Settings should also consider their employer, health and safety, equality, safeguarding, behaviour and staff wellbeing responsibilities.

Settings should apply national guidance according to their type of provision, employer and governance arrangements. Depending on the circumstances, they may also need to seek advice from their employer, HR or personnel provider, the LADO, the police, their data protection officer or legal services.

This document provides general guidance and is not a complete or definitive statement of the law or a substitute for advice about an individual situation. Settings should seek appropriate safeguarding, HR, police or legal advice where necessary.

2. Responding to concerns raised on social media

Each situation will be different and may involve a range of factors. Leaders should consider the nature, context and impact of the content, any immediate risk of harm, the needs of those affected and the policies or procedures that may apply.

This section outlines the key steps leaders and managers should consider when responding to complaints, criticism or other concerns raised on social media. Depending on the circumstances, this may include following the setting's complaints, safeguarding, allegations, behaviour, staff conduct, grievance, health and safety or employment procedures.

The DfE has published a flowchart for schools [responding to online bullying or harassment of staff](#). This is signposted in the flowchart in Appendix One. Settings should also follow the relevant sections of this guidance where concerns involve children/learners, parents, safeguarding allegations or other members of the community.

Distinguishing criticism, bullying and harassment

Not every negative comment, complaint, professional disagreement or difficult interaction will constitute bullying or harassment. Leaders should consider the nature, context and impact of the behaviour, whether it forms part of a pattern, and the circumstances of those involved.

For the purposes of this guidance:

- **Bullying** is unwanted behaviour that may be repeated or, depending on its nature and impact, may involve a serious one-off incident. There is no single legal definition of bullying, so settings should apply the definitions and procedures set out in their relevant policies.
- **Harassment** is unwanted conduct that has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment. Harassment may be related to a protected characteristic under the Equality Act 2010.
- **Online bullying or harassment** may include threatening or abusive messages, trolling, online shaming, hate sites or groups, abusive polls, fake accounts, impersonation, misuse of a person's online identity, unauthorised filming, or manipulated and deepfake content. This is not an exhaustive list.

Reasonable criticism, a complaint raised appropriately, respectful disagreement, constructive feedback or fair management action should not automatically be characterised as bullying or harassment. Further advice can be found at [Definitions of bullying and harassment](#).

Respond calmly and proportionately

Parents, carers and members of the public are entitled to hold and express opinions about education settings, including views that may be negative or critical. Such comments are not necessarily unlawful and cannot always be prevented or removed.

Leaders should consider the nature, context and impact of the content before deciding whether action is required. A response may be necessary where content targets an individual, causes or risks harm, or includes threats, harassment, discriminatory or hate-related abuse, potentially unlawful communications, or information that may breach statutory reporting restrictions concerning an allegation against a teacher. Where the legal position is unclear, settings should seek police or legal advice.

The appropriate response will depend on the circumstances and may involve the setting's complaints, safeguarding, allegations, behaviour, staff conduct, grievance, health and safety or employment procedures. Where it is safe and appropriate, an offline discussion with those involved may help clarify the concerns and identify a constructive way forward.

In some cases, leaders may decide that no immediate action is necessary and that the most proportionate response is to monitor the situation. The reason for this decision should be recorded, together with any agreed review arrangements. Relevant evidence should still be preserved in case the content continues, changes or forms part of a wider pattern.

Preserve and record relevant information

When a setting becomes aware of online content that may affect an individual or the wider community, an appropriately authorised person should preserve relevant information so that the concern can be understood and an appropriate response considered.

Where it is appropriate and lawful to do so, this may include:

- screenshots or copies of the content
- the name of the platform and a link or URL
- account names, usernames and profile details
- the date and time the content was posted or viewed
- relevant comments, replies, shares or other interactions
- the context in which the content appeared
- details of how and when the concern was brought to the setting's attention

An unaltered evidential copy should be preserved securely. If a working copy needs to be shared with those managing the concern, unrelated personal information may be minimised or redacted where appropriate. Names or contextual information should not be removed from the unaltered copy where this may be relevant to a later safeguarding, disciplinary, police or legal enquiry.

Where content has been shared within a private account, closed group or group chat, leaders should consider how the information was obtained and whether it is necessary and appropriate for the setting to retain or use it. The identity of the person who brought the concern to the setting's attention should be protected as far as possible, although confidentiality should not be promised where information may need to be shared for safeguarding, procedural or legal reasons.

Any enquiries should be necessary, proportionate, appropriately authorised and limited to information lawfully available to the setting. Staff should not use personal accounts, false identities or covert methods to gain access to private content. Online connections, follows, likes, comments or group membership should not, on their own, be treated as evidence that a person created, controlled or endorsed an account or its content.

Staff, governors and trustees should not respond to, share or become involved in online discussions about the concern, as this may increase its visibility, escalate the situation or compromise the setting's response. Leaders should ensure that staff know how to report concerns and preserve relevant information without engaging with the content. Further information is provided in Section Four, Preventative Action.

Where there is a possible safeguarding implication, the concern should be shared with the Designated Safeguarding Lead (DSL) at the earliest opportunity.

Do not delay urgent reporting, safeguarding or safety action while gathering information. Screenshots and other records may be helpful, but their absence should not prevent a person or setting from reporting threatening, stalking or harassing behaviour or seeking urgent support.

Do not create, copy, download, print, save or share child sexual abuse material. Such content must be reported immediately in accordance with the setting's safeguarding procedures and appropriate specialist advice should be sought.

Identify who will lead the response

The school, setting, trust or employer should identify an appropriate person to coordinate the response and any investigation.

This decision should take account of:

- who is affected and who is alleged to be responsible
- whether the concern involves a child/learner, parent or carer, staff member, governor, trustee or unidentified person
- whether the headteacher, manager or usual nominated lead is affected or has a conflict of interest

- the need for appropriate independence in any investigation and subsequent review or appeal
- the safeguarding, HR, behaviour, complaints, staff conduct, health and safety and employment responsibilities that may apply
- whether specialist advice or support is required

The person coordinating the response should not be described as the investigator unless a formal investigation is required. Some concerns may be resolved through clarification, support, monitoring, a complaints response or another proportionate action without a formal investigation.

Where the headteacher, manager or nominated lead is the person affected, is the subject of the concern or has another conflict of interest, the matter should be escalated in accordance with the employer's procedures. An appropriate governor, trustee, trust executive, local authority representative or independent person may need to manage the response.

Record keeping

A clear and proportionate record should be maintained. Depending on the nature of the concern, this should include:

- the date the concern was received and how it came to the setting's attention
- the person or people affected
- the reported content or behaviour and its impact
- any immediate risk or safeguarding considerations
- the support offered to those affected
- whether bullying, harassment, discrimination, safeguarding, staff conduct or potentially criminal concerns were considered
- the policies and procedures considered or applied
- the person appointed to coordinate the response
- any conflict-of-interest considerations
- any risk assessment or safety measures
- relevant information or evidence preserved
- referrals, reports and specialist advice sought
- decisions made and the reasons for them
- relevant communication with those affected
- the outcome, any review arrangements and preventative action

Records should distinguish between:

- what has been reported
- what has been observed or verified
- the views or explanations of those involved
- professional assessments and decisions

Records should be accurate, factual and respectful. Avoid speculative, emotive or legally definitive language, particularly where the circumstances have not yet been established.

Records should be stored securely and retained in accordance with the relevant safeguarding, HR, behaviour, complaints, staff conduct, data protection and records-management arrangements. Access should be restricted to those who need the information for an appropriate purpose.

Supporting those affected

Supporting staff

Where a member of staff is targeted online, leaders should consider the matter as a potential workforce safety and wellbeing concern, not solely as a complaint or reputational issue. Employers should take reasonable steps to [provide a safe workplace and safe system of work](#), including protecting staff's mental as well as physical health.

The response should be discussed and, wherever possible, agreed with the affected member of staff. Depending on the circumstances, it should include:

- an immediate check on their safety and wellbeing
- consideration of whether a workplace risk assessment or other safety measures are required
- a nominated point of contact who will provide appropriate updates
- consideration of workload adjustments or other practical support
- access to HR, an employee assistance programme, occupational health, a recognised trade union or other support
- preservation of relevant evidence without repeatedly exposing the staff member to harmful content
- a clear explanation of how the concern will be considered, including any reporting, investigation or escalation arrangements
- opportunities for the staff member to share their views and identify any further support they may need
- consideration of whether the concern indicates a wider, repeated or emerging risk affecting other members of staff
- an agreed point at which the support and any safety arrangements will be reviewed

Leaders should avoid placing responsibility on the affected staff member to monitor the content, respond to those involved or gather further evidence. Any actions taken on behalf of the staff member should be discussed with them wherever possible, unless urgent safeguarding, safety, police or legal considerations require otherwise.

If the affected person is the headteacher, manager or usual nominated lead, the employer, governing body or trust should ensure that another suitably independent person coordinates the response.

Whether and how to inform a staff member who is not already aware of the content should be considered carefully. The decision should take account of:

- the nature and credibility of the content
- any immediate or continuing risk
- the likely impact of informing or not informing the staff member
- whether the staff member needs to participate in the response
- whether the content is likely to become more widely known
- any safeguarding, HR, police or legal advice received

Information should be shared sensitively and only to the extent necessary. The affected staff member should not be shown harmful or distressing content unnecessarily.

Staff may wish to seek advice or support from their recognised trade union or professional networks. In Kent, [KALE](#) have peer support available for school leaders. Support is also available through [Education Support](#) and the UK Safer Internet Centre's [Professional Online Safety Helpline](#) (POSH).

Where online content raises a concern or allegation that may meet the harm threshold, the setting should follow its allegations procedures and contact the LADO in accordance with local arrangements. This includes circumstances where a person working with children may have:

- behaved in a way that has harmed, or may have harmed, a child
- possibly committed a criminal offence against or related to a child
- behaved towards a child or children in a way that indicates they may pose a risk of harm
- behaved, or may have behaved, in a way that indicates they may not be suitable to work with children

Concerns that do not meet the harm threshold should be managed in accordance with the setting's low-level concerns procedures. Where the appropriate threshold or response is unclear, the setting should seek advice from the LADO before beginning any internal investigation that could compromise the allegations process.

Additional resources, links and support

- The [Professionals Online Safety Helpline \(POSH\)](#) has useful guidance.
- POSH have published '[Responding to Online Reputational Issues and Harassment Directed at Schools and School Staff](#)' which may be helpful for leaders.
- Childnet Teacher Guidance: www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- The DfE: [Preventing and tackling bullying and harassment of school staff](#)
- The DfE's [Resources and organisations for further support](#) brings together further guidance and sources of support relating to staff safety, bullying and harassment, online safety, reporting incidents, parental engagement, complaints and staff wellbeing.

Supporting other members of the community

Online content may target a child, parent, carer or another member of the setting community, rather than a member of staff. Leaders should consider the safety and wellbeing of anyone affected, while recognising the limits of the setting's role and its ability to resolve disputes that primarily take place between adults outside the setting.

Where online comments involve parents or carers, leaders should consider:

- whether the content is affecting a child or the safe and effective operation of the setting
- whether mediation or an offline discussion would be safe, appropriate and likely to help
- whether the matter should be addressed through the setting's complaints procedure, parental code of conduct or other relevant arrangements
- what support may be needed by those affected
- whether there is a risk of escalation, confrontation or harm
- whether safeguarding, police or other specialist advice is required

Settings should not routinely become involved in private disputes between adults. However, a proportionate response may be necessary where online behaviour affects a child/learner, targets members of the setting community, disrupts the safe operation of the setting or creates a risk of harm.

Where comments are made about a child/learner, leaders should consider the possible safeguarding impact, including emotional harm, damage to relationships, bullying, discrimination and risks to physical safety. A child/learner may be unaware of the content or may become aware of it through other children/learners, adults or wider online sharing. Whether and how to inform a child should be considered carefully, taking account of the child/learner's age, understanding, wishes and best interests. Children/learners should not be shown harmful or distressing content unnecessarily.

Online discussion and associated conversations within the community may cause significant distress to children. Where there is a safeguarding concern, the setting should follow its child protection procedures and provide appropriate support. Depending on the circumstances, this may include:

- speaking individually with affected children/learners and families
- undertaking proportionate work with a group of children/learners or the wider community
- addressing relevant issues through the curriculum or pastoral provision
- monitoring for further bullying, discrimination or escalation
- involving external agencies where appropriate

Any wider communication or educational activity should avoid identifying those involved, repeating harmful content or drawing unnecessary attention to the issue.

Where content includes a credible threat or indicates an immediate risk of harm, leaders should seek police advice through the appropriate route. Contact 999 where there is an immediate danger. The absence of screenshots or other evidence should not delay urgent safeguarding or safety action.

Kent schools who are unsure how to respond may seek advice through their [Assistant Director for Education](#) or other relevant safeguarding, employer or professional support arrangements.

Discriminatory bullying and harassment

Online abuse connected with an actual or perceived protected characteristic, or with a person's association with someone who has a protected characteristic, should be recognised and addressed explicitly. This may include racist, antisemitic, anti-Muslim, disablist, homophobic, biphobic, transphobic, sexist or age-related abuse.

Leaders should consider:

- the affected individual's experience, wishes and support needs
- the nature, context and impact of the behaviour, including the possible cumulative effect of previous discrimination
- whether the behaviour may constitute discrimination or unlawful harassment under the Equality Act 2010
- whether hostility or prejudice related to the person's identity indicates a possible hate crime or other potentially criminal conduct
- whether immediate safety measures, reasonable adjustments or other support are required
- whether the concern indicates a wider cultural, repeated or systemic issue
- whether relevant policies, training, curriculum provision or wider organisational practice should be reviewed
- how the concern will be recorded and monitored while protecting confidentiality and avoiding unnecessary identification of those involved

The setting should not attempt to determine whether a criminal offence or unlawful discrimination has occurred. Where appropriate, advice should be sought from HR, the employer, legal advisers, the police or relevant specialist support services.

Where online abuse presents an immediate risk of harm, urgent safeguarding or safety action should be taken. Contact 999 where there is an immediate danger.

Meet with the parent or carer where safe and appropriate

Where it is safe and appropriate, an offline discussion with the parent or carer may help clarify their concerns, explain the impact of the online content and identify a constructive way forward. This may take place face-to-face or through another suitable channel.

A parent or carer may not have fully considered the impact of their comments or may be unaware of, have already used, or be dissatisfied with the setting's complaints procedure. An immediate formal letter may sometimes escalate the situation or be shared more widely online. A direct discussion may therefore be more likely to support a constructive outcome.

Before arranging contact, leaders should consider:

- whether there is any immediate risk of confrontation or harm
- whether the matter may involve a safeguarding concern or potentially criminal conduct
- who should lead the discussion and whether another person should be present
- whether any advice should first be sought from the DSL, LADO, HR, the employer, police or legal services
- whether contact could compromise another process or increase the risk to anyone involved

The headteacher, manager or another appropriate leader should invite the parent or carer to explain their concerns and should listen carefully to any legitimate issues raised. Leaders should explain:

- how the online content has affected, or may affect, individuals and the wider community
- which aspects of the content are causing concern
- how the parent or carer can raise and pursue their concerns through the appropriate procedure
- what action the setting proposes to take
- what action the setting is asking the parent or carer to take
- how and when the matter will be reviewed

The discussion should not be used to prevent legitimate criticism, discourage a safeguarding report or restrict access to the setting's complaints procedure.

Where several parents or carers are involved, leaders should consider how to respond safely and fairly while maintaining appropriate confidentiality. Separate discussions may be necessary. Information about one individual should not be shared with another unless this is necessary and lawful.

Leaders may explain that online messages can be misunderstood, taken out of context or shared beyond their intended audience, including where they were originally posted within a private account or group. The discussion should focus on the specific content, its impact and the appropriate route for resolving the underlying concern, rather than making assumptions about the person's intentions.

Where a copy of the content is shared during the discussion, unrelated personal information should be minimised or redacted as appropriate. The identity of the person who brought the content to the setting's attention should be protected as far as possible. An unaltered evidential copy should be retained securely.

Once relevant information has been preserved, leaders may request the removal of content that identifies, targets or risks causing harm to a child/learner, family, member of staff or another person. The reason for the request should be explained clearly. A request to remove content should not prevent the parent or carer from raising the underlying concern through the setting's complaints procedure or another appropriate route.

If the content is not removed, the setting should consider whether further action is necessary and proportionate. Depending on the circumstances, this may include:

- continuing to monitor the situation
- reporting the content or account to the platform
- seeking advice from the Professional Online Safety Helpline
- taking action under the parental code of conduct, home-school or home-setting agreement, or another relevant policy
- reviewing or updating a risk assessment
- seeking safeguarding, LADO, HR, employer, police or legal advice

Any warning, restriction or other action should be necessary, proportionate, recorded and taken in accordance with the setting's procedures. Leaders should not state or imply that legal or police action will follow unless appropriate advice has been obtained and there is a proper basis for doing so.

If the discussion does not resolve the matter, leaders should record the outcome, any areas of agreement or disagreement and the next steps. The setting should continue to consider any legitimate concern fairly while also fulfilling its responsibilities to protect and support those affected by harmful online behaviour.

Where leaders believe that direct contact could increase the risk of confrontation or harm, they should seek appropriate advice before proceeding. If content indicates that a child may be at risk of harm, the setting should follow its child protection procedures and involve other agencies as appropriate.

3. Where concerns remain unresolved or require further action

Where a concern is not resolved through an initial discussion, or where the circumstances require a different or more formal response, the setting should review the information available and decide what further action is necessary and proportionate.

This should take account of:

- any legitimate complaint or concern that remains unresolved
- the nature, context and impact of the online content
- the safety and wellbeing of those affected
- whether the behaviour is continuing or escalating
- whether any safeguarding, employment, equality or potentially criminal concerns arise
- the relevant policies and procedures
- any specialist advice received

The setting should avoid escalating the matter unnecessarily. However, it should take appropriate action where individuals remain at risk, harmful behaviour continues or further support or intervention is required. Decisions and the reasons for them should be recorded.

Arrange a further meeting

A further meeting may be helpful where concerns remain unresolved, agreed actions have not been completed or the online behaviour continues. The meeting may take place face-to-face or through another appropriate channel.

Depending on the setting's governance and employer arrangements, an appropriate governor, trustee, committee member, trust representative or other senior person may attend. Care should be taken not to involve someone whose independence may be required at a later stage of a complaints, grievance, disciplinary or appeal process.

The purpose of the meeting should be to:

- review the concerns raised
- listen to and consider any legitimate complaint
- discuss the impact of the online content
- clarify the setting's expectations and applicable procedures
- review any previous actions or agreements
- identify whether further action or support is required
- agree and record next steps, responsibilities and review arrangements

Anyone attending on behalf of the setting should be appropriately briefed but should receive only the information necessary for their role.

If the parent or carer does not attend or does not wish to meet, the setting may communicate its concerns and proposed next steps in writing. The relevant template letter in Appendix Three may be adapted for this purpose. It should not be used automatically, and any wording should reflect the individual circumstances.

Report content to the platform

Once relevant information has been preserved, the setting may report content or an account to the platform where it was posted. This submits the matter for assessment against the platform's applicable terms, policies and reporting criteria.

Reporting arrangements vary between platforms and may change. Settings should use the platform's current reporting or help processes and retain any confirmation, reference number or response received.

Reporting does not guarantee that content will be removed. There may be a delay before a report is reviewed, and removal may not prevent further content or accounts from being created.

Where content is not removed, a report has not received an appropriate response or specialist support is required, settings may seek advice from the [Professional Online Safety Helpline](#) (POSH) or use [Report Harmful Content](#). Report Harmful Content provides advice about reporting harmful content and may assist with escalation after content has first been reported to the relevant platform.

Settings should use the appropriate reporting route for the type of content involved. Report Harmful Content does not accept reports of sexual images involving anyone under 18 and directs these reports to the [Internet Watch Foundation](#).

Seek further advice

Specialist advice may be required at any stage. The timing and source of advice should reflect the nature and urgency of the concern.

Legal and employment advice

Leaders may seek advice from their employer, HR or personnel provider, recognised trade union or legal adviser.

Formal legal action should not normally be the first response to criticism or a legitimate complaint. However, early legal advice may be appropriate where there are:

- serious or credible threats
- significant safety concerns
- possible reporting restrictions
- disclosure of private or confidential information

- complex employment or governance matters
- sustained conduct causing significant harm
- uncertainty about the setting's legal responsibilities

Following legal advice, a solicitor may write to the person responsible to explain the setting's concerns, any relevant legal implications and the action being requested. Leaders should consider carefully whether formal correspondence is necessary and proportionate, as it may escalate the situation.

The [DfE guidance](#) confirms that it is not a definitive statement of the law or a substitute for legislation and advises employers to seek legal advice where necessary.

Allegations concerning a person working with children

Where online content raises a concern or allegation that may meet the harm threshold, the setting should follow its allegations procedures and contact the LADO in accordance with local arrangements.

Concerns that do not meet the harm threshold should be managed under the setting's low-level concerns procedures. Where the threshold or appropriate response is unclear, advice should be sought from the LADO before beginning internal enquiries that could compromise the allegations process.

Police advice

Police advice should be sought where content may constitute a criminal offence or presents a risk to safety. This may include credible threats, stalking, persistent harassment, hate-related abuse or other potentially unlawful communications.

The setting should use the appropriate police reporting route. Contact 999 where there is an immediate danger or threat of harm. Any police reference number and advice received should be recorded, together with the action taken by the setting.

Urgent reporting should not be delayed while further evidence is gathered. Settings should avoid stating that a criminal offence has occurred unless this has been determined by the appropriate authority.

Safeguarding children/learners

Where online content raises a concern about a child's safety or wellbeing, the DSL should be informed promptly, and the setting should follow its child protection procedures. External agencies should be involved where appropriate. In Kent, this may include making a request for support through the Front Door Service. Immediate safeguarding action should not be delayed while the setting considers a complaint, platform report or wider communication.

Safeguarding adults

Where online content indicates that an adult may be at risk of abuse or neglect, the setting should follow the appropriate adult safeguarding procedures and seek advice or make a referral where required.

Media interest

Where an issue is likely to attract local or national media attention, the setting should consider obtaining communications advice and preparing an agreed, factual response.

Any communication should:

- protect confidentiality
- avoid identifying children or affected individuals unnecessarily
- avoid repeating or amplifying harmful content
- not compromise a safeguarding, police, LADO, complaints, grievance or disciplinary process
- identify an agreed person to respond to media enquiries

Support may be available from the setting's trust, employer, local authority, legal adviser or recognised trade union. Kent education settings may seek advice through the [KCC Media Hub](#).

Concerns raised by members of the public

Online concerns may be posted by a friend or family member of a parent or carer, someone with another connection to the community or a person whose connection to the setting is not known.

The setting's ability and responsibility to intervene will depend on the circumstances. Action is not limited to situations where content is criminal or breaches a platform's terms.

Leaders should consider whether the content:

- affects the safety or wellbeing of a child/learner, staff member or another person
- disrupts the safe or effective operation of the setting
- identifies or targets members of the community
- raises a safeguarding, equality or potentially criminal concern
- requires a complaint or other legitimate concern to be considered
- should be reported to the platform
- requires monitoring or specialist advice

A direct response will not always be necessary or helpful. Where no immediate action is required, leaders may decide to preserve relevant information, record the decision and monitor the situation. Any review arrangements or circumstances that would trigger further action should also be recorded.

Where the person is known to a parent or carer, it may be appropriate to discuss the concern with that parent or carer. However, the setting should not assume that the parent or carer controls or endorses the actions of another adult.

Where the person cannot be identified, the setting may report the content or account to the platform and seek advice from the Professional Online Safety Helpline where appropriate. The setting should avoid speculative attempts to identify the person or assumptions based solely on account connections, followers, likes or comments.

Where content includes a credible threat, indicates a risk to safety or may be criminal, police advice should be sought through the appropriate route.

Concerns raised by children/learners

Comments or concerns shared online by children/learners may involve the setting, other children/learners or members of staff. These situations should not be treated solely as complaints or behaviour matters. They should be considered through a safeguarding lens and in accordance with the setting's child protection procedures.

Leaders should:

- ensure the concern is shared with the DSL promptly
- listen to and record the child/learners account in their own words
- consider what the child/learner may be communicating through the content
- consider the safety and wellbeing of all children/learners involved, including those posting and those affected
- avoid assuming that the child/learner's concern is invalid because it was raised online
- respond through the relevant child protection, behaviour, and anti-bullying procedures
- provide appropriate support, education and proportionate consequences
- consider the child/learner's age, understanding, needs and individual circumstances
- involve parents, carers or external agencies where appropriate and safe to do so

Where the content indicates possible abuse or a risk of harm, the setting should follow local safeguarding procedures and involve external agencies as appropriate.

Where a child/learner makes an allegation about a person working with children, the setting should follow its allegations procedures. The LADO should be contacted where the allegation may meet the harm threshold, or where advice is required because the appropriate threshold or response is unclear.

Children/learners may not fully understand the impact, permanence or reach of online content. The response should therefore combine safeguarding and support with fair, consistent and proportionate action. It should also consider the child/learner's lived experience and any underlying need, vulnerability or peer dynamics.

Concerns raised by staff

Members of staff may share concerns online or become involved in online discussions about the setting, colleagues or leadership decisions. Staff are entitled to hold and express personal views, but remain responsible for complying with relevant professional expectations, confidentiality requirements, the staff behaviour policy or code of conduct, and acceptable use arrangements.

Where concerns are raised by staff online, leaders should:

- avoid responding publicly or becoming involved in online discussions
- preserve relevant information where necessary
- consider the nature, context and impact of the content
- identify any legitimate concern, grievance or protected disclosure
- apply the appropriate grievance, whistleblowing, staff conduct, disciplinary or safeguarding procedure
- identify an impartial person to coordinate or investigate the matter
- seek HR, employer, union or legal advice where appropriate
- ensure that the staff member is treated fairly and given an opportunity to respond

Concerns about a staff member's own treatment, including personal experiences of bullying or harassment, should generally be addressed through the setting's grievance or dignity-at-work procedure.

Whistleblowing procedures apply where a worker raises a concern about serious wrongdoing that they reasonably believe is in the public interest. A concern may involve both a personal grievance and a whistleblowing disclosure. Where this is unclear, the setting should seek HR or legal advice rather than dismissing the concern because it has been raised online.

Where the concern involves another staff member, leader, governor or trustee, the employer should identify an appropriately impartial person to manage or investigate the matter. Consideration should also be given to who could conduct any later review or appeal.

Where online content raises:

- an allegation that may meet the harm threshold, the allegations procedure should be followed and the LADO contacted
- a concern that does not meet the harm threshold, the low-level concerns procedure should be followed
- a possible breach of professional standards, confidentiality or the staff behaviour policy, the relevant employment procedures should be considered
- a safeguarding concern about a child, the DSL should be informed promptly

Settings should balance the need to uphold professional standards with a fair and proportionate response. Online communication may lack context or be open to different interpretations, so conclusions should not be reached until the available information and the staff member's account have been considered.

4. Preventative Action

Education settings cannot prevent every negative comment, complaint or disagreement from being shared online, and content cannot always be removed. Preventative work should therefore focus on:

- creating accessible and trusted routes for raising concerns
- promoting respectful and responsible online behaviour
- protecting and supporting children, staff and other members of the community
- ensuring that relevant policies and procedures are clear and consistent
- preparing leaders and staff to respond calmly and proportionately
- identifying patterns, emerging risks and opportunities for learning

The aim should not be to prevent legitimate criticism or discourage complaints. It should be to support concerns to be raised constructively, reduce the risk of harmful online behaviour and achieve the best possible outcomes for children and the wider setting community.

Employer and governance oversight

Governing bodies, trust boards and other employers should assure themselves that:

- staff have clear and accessible routes for reporting bullying, harassment and other online concerns
- concerns are assessed and responded to promptly, fairly and consistently
- relevant policies address online behaviour and abuse, harassment or intimidation by third parties
- suitable safety, wellbeing and practical support is available to affected staff
- appropriate reporting, escalation and review arrangements are in place
- leaders can access suitable safeguarding, HR, legal, governance and communications advice
- roles and responsibilities are clear where the headteacher, manager or usual nominated lead is affected or has a conflict of interest
- patterns, repeated incidents and emerging risks are identified and reviewed
- learning from incidents informs policies, training, risk assessments and wider preventative work

Information provided for governance or employer oversight should normally be anonymised or thematic. Serious incidents, threats to safety or evidence of a material, repeated or systemic concern should be escalated promptly in accordance with the setting's agreed procedures.

The [DfE guidance](#) expects employers to develop procedures for preventing and addressing bullying and harassment and to ensure that staff are supported, respected and protected.

Build a whole community approach to positive online behaviour

Settings should regularly promote safe, respectful and responsible online behaviour through newsletters, websites, induction arrangements, parent and carer engagement, curriculum provision and other appropriate communications. Adaptable examples are provided in Appendix Three.

Communications should:

- acknowledge that parents, carers, children/learners and staff are entitled to express opinions and raise legitimate concerns
- explain how to contact the setting and raise a concern or complaint
- encourage respectful communication, including where there is disagreement
- ask members of the community to consider the impact before posting or sharing content
- discourage content that identifies, targets, threatens, intimidates or humiliates others
- reinforce the importance of protecting children/learners and adults' privacy
- promote positive adult role-modelling of online behaviour
- explain where online safety advice and support can be obtained

Where a specific incident has occurred, leaders should consider whether wider communication is necessary and proportionate. Wherever possible and appropriate, those directly involved should be contacted before a general communication is issued. Wider communications should not identify individuals, repeat harmful content or compromise a safeguarding, police, LADO, complaints, grievance or disciplinary process.

General communications should not suggest that critical or unpleasant comments are automatically unlawful. Where content includes credible threats, persistent harassment, discriminatory abuse or other potentially unlawful behaviour, the setting should seek appropriate safeguarding, police or legal advice.

Settings should make their communication and complaints routes easy to find and use. Parents and carers should know:

- who to contact initially
- how to raise a formal complaint
- where the complaints procedure can be accessed
- how concerns will be acknowledged and considered
- what to do if they remain dissatisfied
- how to raise an urgent safeguarding concern

Settings may also remind members of the community that social media platforms have reporting processes for content that may breach their applicable terms or policies. Reporting does not guarantee removal, and users should be directed to current platform guidance rather than settings attempting to describe individual reporting processes in detail.

Supporting staff to manage their online safety

Staff should receive appropriate safeguarding and online safety training in accordance with the version of *Keeping children safe in education* currently in force and the requirements applying to their setting.

Settings should help staff understand how professional expectations, personal online activity and digital security may affect their safety, privacy and professional role. This should be addressed through induction, regular training, the staff behaviour policy or code of conduct and acceptable use arrangements.

Settings should:

- encourage staff to use school or setting contact details and accounts for work-related business and to keep personal and professional communications separate
- remind staff not to accept social media friend or follow requests from current or past learners or their families
- ensure staff seek senior guidance where contact with learners or their families could create professional-boundary concerns, for example, where there are pre-existing relationships
- encourage staff to review the privacy and security settings of personal accounts regularly
- remind staff that content posted or shared by family members, friends or colleagues, including content in which they are tagged, may affect their privacy
- ensure staff understand that privacy settings cannot guarantee that content will remain private
- ensure staff know not to respond or retaliate if they are targeted online
- make clear how staff should preserve relevant information, report a concern and access support
- avoid placing responsibility on affected staff to monitor harmful content or investigate who is responsible

Staff should not be expected to withdraw unreasonably from normal online activity. Preventative advice should be proportionate and should not transfer responsibility for harmful behaviour onto the person affected.

Further advice is available in the DfE's [Online safety guidance for staff](#).

Acceptable Use of Technology Policies (AUP)

Settings should have appropriate acceptable use arrangements that establish clear expectations for the safe, responsible and professional use of technology by staff and children/learners.

Acceptable use arrangements should:

- be appropriate to the age, understanding and needs of the intended users
- explain expected and unacceptable use clearly
- cover relevant devices, systems, online services, social media and emerging technology
- explain how concerns or breaches should be reported
- identify possible responses to misuse without predetermining sanctions
- link with safeguarding, behaviour, anti-bullying, staff behaviour, online safety, data protection and disciplinary procedures
- be communicated in an accessible form
- be reviewed regularly and following significant incidents or technological developments

Staff and children/learners should be supported to understand the arrangements and what they mean in practice. Settings may use signatures or digital acknowledgements to confirm that policies have been read and understood, but a signature alone does not demonstrate understanding or ensure compliance.

Parents and carers may also be asked to support the setting's approach to online safety and reinforce safe and respectful technology use outside the setting. Expectations should be realistic and should not imply that the setting can control all family technology use or online activity outside its remit.

LESAS AUP templates can be found on [our website](#).

Example statements:

I will support the school/setting approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text and video online responsibly.

I will support my child to use technology safely and responsibly and not to create, post or share content that threatens, targets, bullies, harasses or risks causing harm to another member of the setting community.

Setting policies and procedures

The setting's policies should provide a consistent framework for preventing and responding to online concerns. Relevant documents may include:

- child protection
- behaviour and anti-bullying
- staff behaviour or code of conduct
- acceptable use of technology
- complaints
- whistleblowing
- grievance and dignity at work
- allegations and low-level concerns
- disciplinary procedures
- parental code of conduct, home-school/setting agreements
- data protection, confidentiality and information security
- health, safety and staff wellbeing
- communications and media

Settings should follow the complaints requirements and guidance applicable to their type of provision. Maintained schools should have regard to the DfE's [guidance for maintained schools](#). Academies, independent schools and other providers should follow the requirements and procedures applying to them.

Policies should be accessible, use consistent terminology and clearly identify:

- expected standards of conduct
- routes for reporting concerns
- who will coordinate different types of response
- how conflicts of interest will be managed
- the support available to affected people
- when concerns may require external advice or referral
- how decisions and outcomes will be recorded and reviewed

Where parents or carers raise concerns, the setting's complaints procedure should be followed. The procedure should be easy to locate on the setting's website and available in an accessible format. Relevant policies and routine communications should signpost parents and carers to it. Settings may also signpost families to [Parentkind's guide to raising concerns with a child's school](#), where relevant to the setting.

Where concerns involve children/learners, they should not be treated solely as complaints. Leaders should consider the child/learners safety, welfare, wishes and lived experience and respond through the setting's child protection, behaviour, and anti-bullying procedures as appropriate.

Settings should ensure that their staff behaviour policy or code of conduct addresses the acceptable use of technology, staff-child relationships and communications, including the use of social media. The setting may maintain a separate social media policy or integrate expectations into existing policies, provided responsibilities and reporting routes remain clear.

Supporting staff to raise concerns

Settings should promote a culture in which staff feel able to raise concerns safely and through appropriate routes. Staff should have access to:

- routine line-management and supervision arrangements
- grievance or dignity-at-work procedures for concerns about their own treatment
- safeguarding and allegations procedures
- low-level concerns procedures
- whistleblowing arrangements for serious wrongdoing reasonably believed to be in the public interest
- HR, union or other professional advice where appropriate

These routes should be clearly communicated, accessible and supported by timely and proportionate responses.

Leaders should not assume that every concern posted online is a disciplinary matter or that using social media makes an underlying concern invalid. The content, context, professional expectations and any legitimate grievance, safeguarding concern or protected disclosure should all be considered fairly.

A concern may include both a personal grievance and a potential whistleblowing disclosure. Where the appropriate route is unclear, HR or legal advice should be sought.

Parental codes of conduct and shared expectations

Where appropriate, settings may use a parental code of conduct, home-school or home-setting agreement, or another shared statement of expectations to promote respectful communication and positive online behaviour.

These arrangements may include expectations that parents and carers will:

- raise concerns directly through the setting's communication or complaints routes
- communicate respectfully with staff, children and other families
- avoid posting or sharing content that identifies or targets individuals
- protect confidential and personal information
- model safe and responsible online behaviour
- support children to use technology safely and appropriately

These documents should not be described as automatically creating a contract or as giving the setting unrestricted authority over parents' private online activity. Any action taken in response to a breach should have a clear basis in the setting's procedures and should be necessary, fair and proportionate.

The agreement should not:

- prevent legitimate criticism or complaints
- discourage reporting a safeguarding concern
- restrict lawful communication
- imply that parents are responsible for content posted by another adult
- promise enforcement action that the setting cannot take

Example statements:

"Parents/carers will support the school/setting approach to online safety and will not upload, share or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school/setting community".

"Parents and carers are encouraged to use the setting's established communication and complaints routes when raising concerns. We ask families not to post or share information that identifies, targets or risks causing harm to children, families or members of staff."

"If at any time during your child's time at xxxx school/setting, you wish to make a complaint, then you are advised to follow the school's complaints procedure, which can be found on the school website [insert link]. We ask parents and carers not to share confidential or sensitive information about children, families or staff on social media and to raise concerns directly through the setting's communication or complaints routes"

Promote positive use of social media

Official social media channels can support communication, celebrate achievements, share reliable information and strengthen engagement with families. Their use should form part of the setting's wider communications strategy rather than being presented primarily as a way to prevent complaints.

Where a setting operates an official page, profile, group or other online channel, it should establish:

- a clear purpose and intended audience
- appropriate administration and moderation arrangements

- authorised users and account-security controls
- expectations for comments and participation
- procedures for responding to questions, complaints and harmful content
- arrangements for protecting personal information and obtaining appropriate consent
- continuity arrangements when staff or volunteers leave their role
- routes for reporting safeguarding or urgent concerns outside social media

Parent-teacher associations and similar groups may operate their own online spaces. The setting should be clear about whether a group is official, endorsed, independent or simply associated informally with members of the community.

Where a group uses the setting's name, logo or branding, appropriate permissions and boundaries should be agreed. However, settings should avoid implying that they control independent parent-led groups where this is not the case.

An official account may offer a reliable communication channel, but it will not necessarily prevent unofficial groups, criticism or complaints from emerging. Parents and carers should be directed away from social media when they need to share confidential information, report a safeguarding concern or submit a formal complaint.

Provide accessible routes for raising concerns

Leaders should provide a range of accessible ways for parents, carers, children/learners and staff to raise questions or concerns directly. These may include:

- clearly identified contact details
- a dedicated email address
- opportunities to arrange an appointment
- agreed availability of an appropriate member of staff
- accessible complaints and safeguarding information
- support for people who face communication, language, disability or digital-access barriers
- child-friendly routes through which children can speak to a safe adult
- arrangements for urgent concerns outside normal communication processes

Settings should review whether these routes are understood, trusted and working effectively. Repeated complaints emerging through social media may indicate that communication routes are unclear, inaccessible or not experienced as responsive. This does not excuse harmful online behaviour, but it may identify an opportunity for organisational learning.

5. Responding to Fake, Anonymous and Misleading Accounts, including AI-generated content

Education settings may become aware of social media accounts or online content that uses the setting's name, logo or branding without authorisation, appears to impersonate the setting or another person, or shares misleading, harmful or manipulated content about children, staff or the wider community.

This may include content that is false, exaggerated or likely to cause reputational harm. In some cases, content may also be manipulated or generated using artificial intelligence (AI), such as edited images, synthetic audio or altered videos that appear authentic but are not.

These accounts may claim to represent the setting, use logos or branding, or use provocative or 'baiting' titles to attract attention and encourage others to contribute comments, rumours or further content. Content shared may be inappropriate or harmful, may constitute bullying or harassment and, in some circumstances, may include allegations or potentially unlawful material.

These accounts may be created by a child, parent or carer, staff member, former member of the community or someone with no confirmed connection to the setting. Some may initially be created as a 'prank' or to attract attention through views and followers. However, regardless of intent, the content may have a significant emotional or safeguarding impact on children, staff and the wider community.

Where AI tools have been used to manipulate or generate content, the impact can be particularly harmful because the content may appear credible, increasing the risk of escalation, distress or reputational damage.

These situations can be distressing for settings and the individuals involved. The [Professional Online Safety Helpline](#) has published [advice](#) about [responding to fake accounts online](#). It has also produced a [short video](#) explaining the issue, how educators can report distressing content and how to contact the helpline for further support.

SWGfL have also published [Responding to Online Reputational Issues and Harassment Directed at Schools and School Staff](#). This includes guidance on fake and impersonation accounts, unmanaged community groups, negative online discussion and allegations.

Understanding AI-generated or manipulated content

Settings should be aware that content shared online may not always be genuine, and could be created, altered or amplified using AI tools.

This may include images, audio or videos that have been edited to change their meaning or context, synthetic content designed to imitate identifiable individuals, or content that falsely suggests particular behaviour, actions or events.

It is important that leaders focus on the impact and potential risk of harm rather than attempting to determine the technical authenticity of the content themselves. However, they should avoid making definitive statements about whether content is genuine or artificially created unless this has been reliably established.

Uncertainty about whether content is authentic should not delay necessary safeguarding or safety action. Settings should preserve relevant information, avoid unnecessary redistribution, support those affected and seek specialist advice where required.

Further guidance is available from the UK Online Harms Early Warning Working Group's [*Protecting your setting's images from AI manipulation and abuse*](#). The guidance supports education settings to consider how photographs and videos are managed, shared and protected, how image-security practices can be strengthened, and how to respond where images have been misused or manipulated.

Where content appears to involve identifiable members of the setting community, leaders should consider whether it raises safeguarding concerns, including bullying, harassment, impersonation, allegations or possible abuse, and respond in accordance with the setting's child protection, allegations or other relevant procedures.

AI-generated content should be treated in the same way as other harmful online behaviour; the priority is assessing risk, supporting those affected, and following safeguarding procedures.

Responding to concerns

Each situation will be different and may involve complicating factors. Leaders should consider the nature, context and impact of the content, any immediate risk of harm, the needs of those affected and the procedures that may apply.

Where necessary, advice may be sought from the employer, trust or local authority, the DSL, the LADO, HR or personnel services, legal advisers, the police or the Professional Online Safety Helpline.

The setting should identify an appropriate person to coordinate the response. Depending on the circumstances, this may be the headteacher, manager, DSL or another suitably authorised leader. Where the usual lead is affected or has a conflict of interest, another appropriately independent person should coordinate the response.

Urgent safeguarding or safety action should not be delayed while the setting seeks to establish who created the account or whether the content is genuine.

Preserve relevant information

An appropriate member of the senior leadership team should be identified to preserve and record relevant information so that prompt and appropriate action can be taken. Depending on the circumstances and the potentially sensitive nature of the content, this may be the DSL, headteacher, manager or another suitably authorised leader.

Where online content raises an allegation that may meet the harm threshold, the headteacher or manager should follow the setting's allegations procedures and contact the LADO in accordance with local arrangements. Concerns that do not meet the harm threshold should be managed under the setting's low-level concerns procedures, with LADO advice sought where the appropriate threshold is unclear.

Settings should be mindful that content may be edited, deleted or altered quickly, particularly where AI tools are involved; evidence should therefore be captured as soon as possible.

Where it is appropriate and lawful to do so, settings may:

- take screenshots or copies of the content
- record the platform, account name, username and relevant link or URL
- record the dates and times the content was posted or viewed
- note relevant comments, replies, shares or other interactions
- record how and when the concern was brought to the setting's attention

This information may help the setting build a chronology and identify any patterns of behaviour. Publicly available information about followers, following lists, comments or shared content may provide relevant context. However, following, viewing, liking, commenting on or sharing content does not, by itself, establish that a person created, controlled or endorsed the account.

An unaltered copy of the relevant content should be stored securely, with access limited to those who need it for an appropriate purpose. Where there is uncertainty about whether content can lawfully or safely be copied or retained, the setting should avoid copying, downloading or redistributing it and seek appropriate safeguarding, police or legal advice.

Staff and children/learners reporting concerns should be advised not to respond to, share or become involved in online discussions about the content. Doing so may increase its visibility, escalate the situation or compromise the setting's response. Concerns should be passed promptly to the DSL, headteacher, manager or other identified lead.

Undertake proportionate internal enquiries

Social media platforms will usually only [disclose personal information about account holders where the relevant legal requirements are met](#). The police and social media platforms may therefore be unable to provide information that identifies the person responsible.

Settings may need to undertake proportionate internal enquiries to understand the circumstances, assess risk and determine the appropriate response. Police advice should be sought where the content may be unlawful or presents a risk to safety.

Any internal enquiries should be necessary, proportionate, appropriately authorised and limited to information lawfully available to the setting. Leaders should avoid speculative searches, covert monitoring or assumptions based solely on online connections, follows, likes, comments or reactions.

Fake or anonymous accounts may be created by a child, parent or carer, staff member, former member of the community or someone with no confirmed connection to the setting. Leaders should not make assumptions about responsibility and should base any further action on the available information.

Publicly available account information, including followers, interactions and shared content, may provide relevant context. However, an account connection, follow, like, comment or reaction does not, by itself, establish ownership, involvement or responsibility.

Where there is a clear and proportionate reason to do so, leaders may speak with individuals whose involvement or knowledge may be relevant to understanding the concern. Individuals should be given an appropriate opportunity to explain their involvement or share relevant information. Following, viewing, liking or otherwise interacting with an account should not be treated as evidence that a person created, controlled or endorsed it.

Where internal enquiries do not identify the person responsible, or where wider preventative work would be helpful, settings may consider addressing social media use more generally with the community. Communications should be kept general and should avoid naming or linking to the account, repeating harmful content or drawing unnecessary attention to it. Publicising the account may increase its visibility or contribute to copycat activity.

Where appropriate, settings might explain that an account posting potentially harmful content has been brought to their attention and that the concern is being considered in accordance with the setting's safeguarding, behaviour, online safety and other relevant procedures.

If the issue is addressed through tutor groups, assemblies or other communications with children/learners, appropriate staff should be available to respond to questions, identify emerging safeguarding concerns and provide support to children/learners who may be affected. Staff should not treat children/learner's reactions or behaviour during these discussions as evidence of involvement.

In some cases, settings may explain that further action will be considered if the concern cannot be resolved or if the content raises a safeguarding or safety concern or may be unlawful. This may include seeking specialist, police or legal advice where appropriate. Any communication should be measured and should not imply that police or legal action is inevitable.

Such communication may prompt further information to be shared, the person responsible to come forward or the account to be removed. However, settings should not use the possibility of police or legal action solely as a means of encouraging a disclosure and should continue to follow their agreed procedures.

Leaders should avoid making assumptions about whether content is genuine or artificially created and should not attempt technical verification without appropriate expertise or support. The focus should remain on assessing risk, supporting those affected and taking fair and proportionate action.

Responses where the person responsible has been identified

Where the available information reasonably establishes who is responsible, the setting should give the individual an opportunity to respond before reaching conclusions or deciding what action to take. Any response should be fair, proportionate and in accordance with the relevant safeguarding, behaviour, anti-bullying, staff conduct, disciplinary or other applicable procedures.

The person responsible may not have fully considered the emotional, safeguarding or reputational impact of the content. Even where an account or content was initially created as a joke, experiment or attempt to attract attention, this does not lessen the need to consider its impact on individuals and the wider setting community.

Once relevant information has been preserved, and where it is safe and appropriate to do so, the setting may request that the harmful content or account is removed. The reason for the request should be explained clearly.

Action should be taken in accordance with the setting's relevant policies and procedures.

Depending on the circumstances and the person involved, this may include:

- targeted education and support
- restorative or relationship-based work, where appropriate
- proportionate behaviour consequences or sanctions
- action under the staff behaviour, disciplinary or other employment procedures
- support to understand the impact of the content
- review of any wider safeguarding or safety concerns
- an agreed plan to reduce the likelihood of recurrence

Where a child/learner is involved, the response should take account of their age, understanding, individual circumstances and any underlying needs or vulnerabilities. The child/learner should be given an opportunity to explain what happened, including their reasons for creating, posting or sharing the content.

Where there are safeguarding concerns relating to a child/learner or family, additional action may be required. This could include seeking advice, making a request for support or liaising with any relevant professionals already involved, such as social workers or Family Help. The response should not be based solely on whether the child/learner or family is already known to services.

Where AI tools have been used, settings may wish to include education about the ethical and responsible use of technology as part of the response. This should include consideration of authenticity, consent, privacy, the potential impact on others and the ease with which manipulated content can be shared beyond its intended audience.

Any outcome and the reasons for it should be recorded. The setting should also consider whether follow-up support, monitoring or wider preventative work is required.

Supporting affected staff and children/learners

Leaders and managers should consider the safety, wellbeing and support needs of everyone affected. Employers should take reasonable steps to protect staff from abuse, harassment or intimidation, including behaviour by parents, carers, children/learners and other third parties, as part of their wider health and safety, wellbeing, equality and risk-management responsibilities.

Where an affected staff member or child/learner is aware of the content, leaders should explain how the setting intends to respond, agree how they will be kept updated and consider what practical or emotional support may be helpful. Care should be taken not to repeatedly expose the person to harmful or distressing content.

Where the person is not already aware of the content, leaders should consider carefully whether it is necessary and appropriate to inform them. This should take account of any immediate risk, the likely impact of informing or not informing them, whether they need to participate in the response and any safeguarding, HR, police or legal advice received.

Staff, including headteachers and managers, may wish to seek support from their recognised trade union, professional networks, employee assistance programme, occupational health service or [Education Support](#). Leaders may also seek advice from their employer, HR or personnel provider, or legal adviser where appropriate.

Any support or safety arrangements should be reviewed if the content continues, spreads or has an increasing impact.

Report and escalate concerns

Where a specific issue has occurred, settings should consider whether communication with staff, children/learners, parents or carers is necessary and proportionate.

Any communication should be accurate, measured and focused on safeguarding and appropriate outcomes. It should avoid identifying those involved, repeating harmful content or drawing unnecessary attention to the account. Leaders should be realistic about what they hope to achieve, as reactive or emotionally led communication may escalate the concern.

Where content presents a risk to safety or may be illegal, including where it has been created or manipulated using AI, the setting should inform the DSL and seek advice from the police or other appropriate agencies. Contact 999 where there is an immediate risk of harm. Settings should avoid making their own determination that a criminal offence has occurred and should not delay urgent action while gathering further information.

Where online content raises an allegation that may meet the harm threshold, the setting should follow its allegations procedures and contact the LADO in accordance with local arrangements, even where the allegation may ultimately be found to be unfounded, false or malicious. Low-level concerns should be managed under the setting's low-level concerns procedures, with LADO advice sought where the appropriate threshold or response is unclear.

Once relevant information has been preserved, the setting may report the content or account through the platform's appropriate reporting process. A platform report can be made whether or not the person responsible is known and whether or not a criminal offence has been established.

Where staff have been targeted through fake, impersonation or manipulated content, they may be able to submit a privacy or impersonation report directly, or the setting may support them to do so. Platforms may also provide reporting routes where the setting's name, logo or other protected material has been used without permission.

Where photographs or videos connected with the setting have been misused or manipulated by AI, settings should also refer to the [Image guidance for education settings](#) for further advice on containment, reporting, support and preventing recurrence.

Reporting does not guarantee removal. Settings should retain any reporting confirmation, monitor the outcome and record any response received. Where content is not removed or continues to have a significant impact, advice may be sought from the Professional Online Safety Helpline. Police or legal advice may also be required where the nature, impact or continued circulation of the content presents a significant concern.

Preventative action

Removal of a harmful or impersonation account may reduce its immediate impact. However, removal does not establish who created the account and may not prevent further or copycat accounts from being created. Settings should therefore also consider appropriate preventative and educational action.

Settings should:

- Review relevant policies to ensure that online behaviour is addressed and that clear procedures for responding to concerns are in place.
- Clarify expectations for learner behaviour and conduct with staff, parents, carers and learners, including expectations regarding the use of mobile technology on site and social media.
- Review curriculum provision to ensure that online safety is embedded within RSHE and other appropriate areas. Education should include healthy and respectful relationships, positive online behaviour and the impact of online actions on others.
- Review staff training and the staff behaviour policy or code of conduct. Ensure that staff know how to report an online concern, what to do if they are targeted and how to access support. Staff should also be encouraged to review the privacy and security settings of their personal accounts regularly.
- Ensure that training, policies and curriculum approaches address emerging risks, including the misuse of AI tools and manipulated or synthetic media.
- Review how photographs and videos are selected, stored and shared through websites, social media and other digital spaces. Consider whether individuals need to be identifiable, whether consent and privacy arrangements remain appropriate, and whether image-security expectations are reflected in staff training and relevant policies.

6. Conclusion

Social media enables opinions, concerns and complaints about education settings to be shared quickly and with a wide audience. While education settings should be prepared to respond robustly to harmful online behaviour, they should also recognise the right of parents, carers, children/learners, staff and members of the public to express opinions, raise legitimate concerns and respectfully disagree.

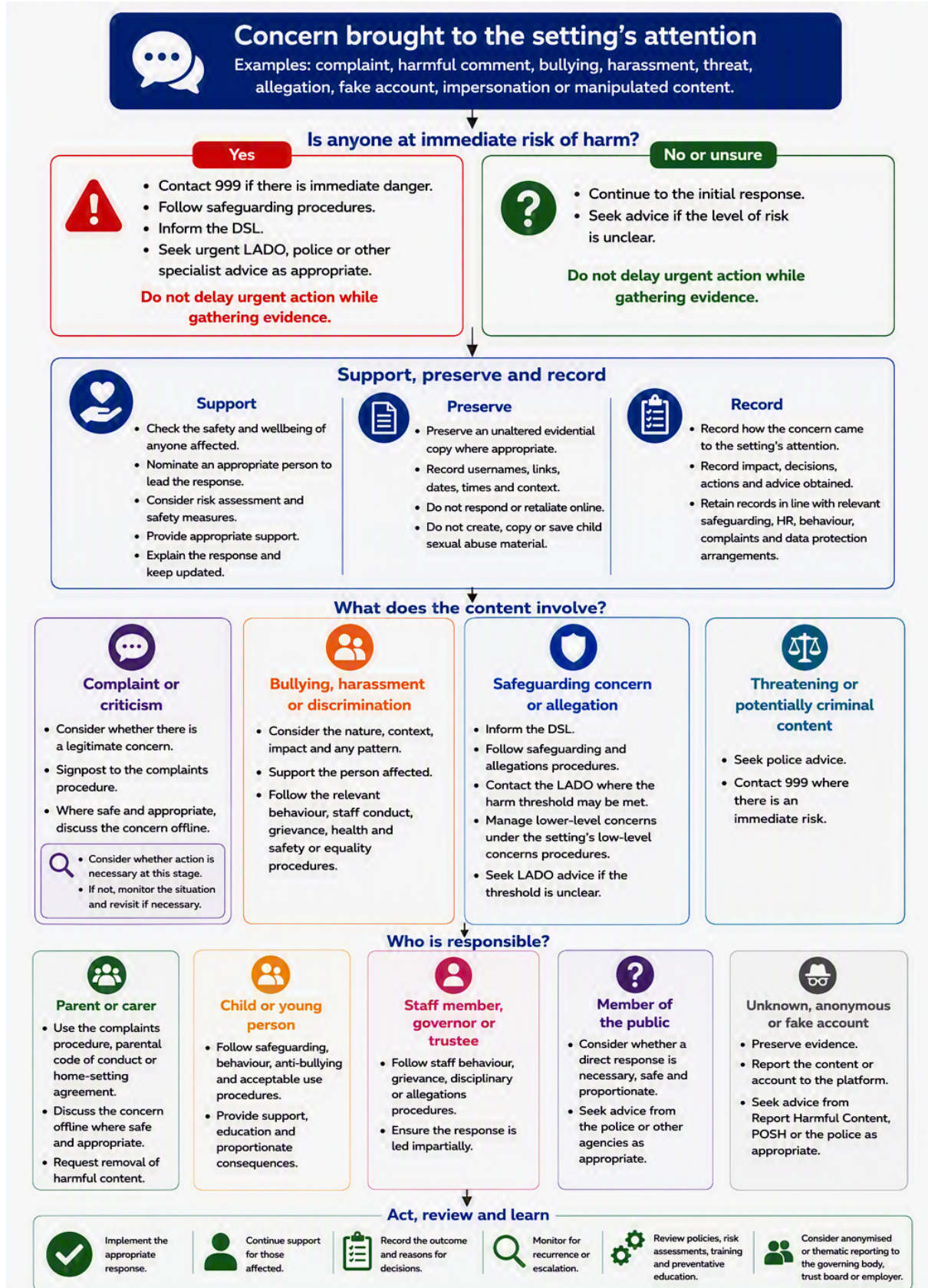
Online content may affect the safety and wellbeing of children/learners, staff and other members of the community. It may also spread incomplete or misleading information and affect confidence in the setting. Leaders should therefore respond calmly, fairly and proportionately, considering the nature, context and impact of the content and using the relevant safeguarding, complaints, behaviour, staff conduct, health and safety or employment procedures.

Education settings cannot prevent every concern or critical comment from being shared online, nor can they ensure that all content will be removed. Preventative work should focus on providing clear and accessible routes for raising concerns, promoting respectful online behaviour, protecting and supporting those affected, and ensuring that staff and leaders are prepared to respond appropriately.

By promoting openness, professional curiosity, positive relationships and responsible use of technology, settings can help their communities raise concerns constructively, learn from incidents and achieve positive outcomes for children/learners and the wider setting community.

Appendix One: Responding to Concerns Flowchart

This flowchart should be read alongside this guidance and the setting's own child protection, allegations, behaviour, complaints, staff conduct, health and safety and employment procedures. The [DfE](#) has published guidance, including a flowchart specifically for work-related online bullying or harassment of school staff.



Appendix Two: Legal Information

Expressions of opinion, criticism and accounts of personal experience will not necessarily give rise to legal action, even where they are negative or upsetting. Whether online content raises a criminal or civil legal issue will depend on the particular facts, context and applicable law.

Settings should not attempt to determine legal liability themselves. Where content includes threats, persistent harassment, discriminatory or hate-related abuse, possible breaches of reporting restrictions, disclosure of private information or another potentially unlawful act, appropriate police or legal advice should be sought.

The DfE has published [Statutory obligations regarding workplace bullying, harassment and safety](#) which provides additional advice and guidance.

The following information provides a brief overview of some legal provisions that may be relevant. It is not legal advice, is not exhaustive and should not be used to determine whether an offence or civil wrong has occurred. Other legislation or legal principles may apply depending on the circumstances.

Criminal concerns

- **Protection from Harassment Act 1997:**
 - Harassment may give rise to criminal or civil proceedings where a person pursues a course of conduct that they know, or ought to know, amounts to harassment. A course of conduct generally involves conduct on at least two occasions. Online posts, messages and other communications may form part of that course of conduct.
 - Available information, such as messages, screenshots, dates and times, may assist the police or another relevant agency. However, reporting should not be delayed while further information is gathered, particularly where there is a risk to safety or wellbeing. Settings should seek police or legal advice where appropriate.
- **Communications Offences:**
 - Online communications may constitute criminal offences depending on their content, purpose, context and impact.
 - Relevant legislation may include the Malicious Communications Act 1988, the Communications Act 2003 and Part 10 of the Online Safety Act 2023. The Online Safety Act 2023 introduced new offences, including false communications and threatening communications, which came into force on 31 January 2024.
 - The Online Safety Act repealed the earlier provisions of the Malicious Communications Act 1988 and Communications Act 2003 dealing with false messages, and the earlier provision of the Malicious Communications Act concerning threatening communications. Other provisions remain relevant to some

grossly offensive, indecent, obscene or menacing communications and persistent misuse of a public electronic communications network.

- The application of these offences is fact-specific. Settings should not attempt to determine whether an offence has been committed and should seek police or legal advice where communications appear threatening, abusive or otherwise potentially unlawful.

- **Stirring up hatred**

- Certain threatening communications intended to stir up hatred may constitute criminal offences under the Public Order Act 1986, as amended.
- The relevant provisions concern conduct intended to stir up hatred on specified grounds. The application of these offences depends on the wording, intention, context and circumstances. Where online content appears to encourage hatred or violence against a person or group, the setting should preserve relevant information appropriately and seek police advice.

- **Reporting restrictions concerning allegations against teachers**

- Section 141F of the Education Act 2002 contains reporting restrictions concerning certain allegations against teachers. The restrictions apply where a person employed or engaged as a teacher at a school is accused, by or on behalf of a registered pupil at that school, of conduct that would constitute a relevant criminal offence.
- Information must not be published if it is likely to lead members of the public to identify the teacher as the person who is the subject of the allegation. The restrictions are subject to specific conditions, exceptions and provisions concerning when they cease to apply. They do not apply to every allegation or every person working in an education setting.
- Where online content identifies, or may identify, a teacher in connection with such an allegation, the setting should avoid repeating or further publishing the information and should seek LADO and legal advice. Relevant information should be preserved securely where it is appropriate and lawful to do so.

- **Intimate image abuse (including AI-generated or 'deepfake' content)**

- It is a criminal offence in the UK to share, or threaten to share, intimate images without consent under legislation including the Criminal Justice and Courts Act 2015 and amendments made through the Online Safety Act 2023 to the Sexual Offences Act 2003. These offences apply to images which are real or appear to be of an individual (including manipulated or AI-generated content).
- The legal position in relation to intimate images and AI-generated or digitally manipulated content continues to develop. Schools and settings should seek up-to-date police, safeguarding or legal advice to determine whether an offence has been committed.

Civil concerns: defamation, privacy and confidentiality

- **Defamation**

- In England and Wales, a statement is not defamatory under the Defamation Act 2013 unless its publication has caused, or is likely to cause, serious harm to the reputation of the claimant. For a body that trades for profit, serious harm requires serious financial loss.
- The Act includes statutory defences, including truth, honest opinion and publication on a matter of public interest. Whether a statement is defamatory and whether a defence applies will depend on the particular facts and context.
- Settings and individuals should not describe content as defamatory, threaten defamation proceedings or demand removal on that basis without first obtaining appropriate legal advice. Criticism, disagreement, an honestly expressed opinion or an account of personal experience will not necessarily be defamatory simply because it is negative or damaging to reputation.

- **Privacy, confidentiality and personal information**

- Where online content shares private, confidential or personal information, there may be data protection, confidentiality, privacy or safeguarding implications.
- The setting should consider:
 - whether anyone is at immediate risk
 - whether the information identifies a child or another vulnerable person
 - whether the setting itself has experienced a personal-data breach
 - whether the content should be reported through the platform's privacy, impersonation or harmful-content process
 - whether advice is required from the setting's data protection lead, employer, personnel provider, safeguarding adviser or legal adviser
- The setting should avoid redistributing the information unnecessarily. Any relevant material retained for safeguarding, employment, police or legal purposes should be stored securely and access should be limited to those who need it for an appropriate purpose.
- Where the concern may involve a personal-data breach by the setting, it should be managed through the setting's data-protection and breach-reporting procedures.
- Schools should also refer to the DfE's Data protection in schools guidance, including its advice on photographs and videos, information sharing, record management, personal-data breaches and generative AI.

Legal provisions and reporting routes may change. Settings should obtain current police or legal advice where necessary and should not rely on this appendix as a substitute for advice about the particular circumstances of a case.

Appendix Three: Template letters

Please be aware that settings must not share any information which could impact or compromise a live investigation, including police investigations; please seek advice before using these templates if this is a possible risk.

Preventative approaches

General Awareness Information for Newsletters

At **[school/setting name]**, we want the best possible outcomes for every child. We recognise that parents and carers may sometimes have questions or concerns or feel that something could have been handled differently.

If you have a concern, please raise it directly with us so that we can listen, understand what has happened and work with you to identify an appropriate way forward. You can do this by **[insert details, for example, speaking with the headteacher/manager, contacting the office or emailing a dedicated address]**.

Sharing concerns on social media can make it more difficult for the setting to understand and respond to the issue. Online comments may also affect children, families and members of staff, including people who are not directly involved.

Our complaints procedure explains how concerns can be raised and considered. It is available **[on our website at [link]/from the school or setting office]**.

Thank you for helping us maintain a safe, respectful and supportive community.
[Name]

[Headteacher/Manager/Chair of Governors or equivalent]

General Awareness Letter for all parents

Dear parents and carers

Working together to promote positive online behaviour

Online safety is an important part of keeping children safe at **[school/setting name]**. We rely on the support of our whole community to ensure that children receive consistent messages about communicating safely, respectfully and responsibly online.

- Parents, carers and other adults play an important role in modelling positive online behaviour. Before posting, commenting on or sharing online content, we encourage everyone to consider:
- whether the information is accurate and appropriate to share
- how the content may be understood by others
- whether it could identify or affect a child, family or member of staff
- whether a concern would be better raised directly with the setting
- the example the online behaviour sets for children

Everyone is entitled to express a view or raise a concern. However, online content that identifies, targets, threatens, intimidates or humiliates another person may cause significant harm and, in some circumstances, may constitute bullying or harassment or raise safeguarding concerns.

If you have a question, concern or complaint about **[school/setting name]**, please raise it directly with us so that we have an opportunity to listen, understand and respond appropriately. Our complaints procedure and other relevant policies are available **[on our website at [link]/from the school or setting office]**.

We ask all members of our community to:

- use the setting's agreed communication and complaints routes
- communicate respectfully, including when expressing disagreement
- avoid sharing information that could identify or target individual children, families or staff
- think carefully about the possible impact before posting or sharing content
- model safe and responsible online behaviour for children

Further advice for families is available from:

- www.ceopeducation.co.uk/parents/
- www.saferinternet.org.uk
- www.childnet.com
- www.nspcc.org.uk/keeping-children-safe/online-safety
- www.internetmatters.org

We value our relationship with parents and carers and want to work together to maintain a safe, respectful and supportive community.

If you would like to discuss an online safety matter or require further information, please contact **[name, role and contact details]**.

Thank you for your continued support.

Yours sincerely

[Name]

[Headteacher/Manager/Chair of Governors or equivalent]



Letters following specific issues

Template incident letter for use with all parents/carers

Do not use this letter if the information could identify an individual or compromise a safeguarding, police, LADO, complaints, grievance or disciplinary process. Wherever possible, speak with the parents or carers directly involved before sending a wider communication. Adapt the wording carefully so that it does not imply that conclusions have been reached before the circumstances have been considered.

Dear parents and carers

Online safety is an important part of keeping children safe at **[school/setting name]**. We need the support of our whole community to ensure that online safety messages are consistent and that everyone communicates safely and respectfully online.

We are aware of recent online discussion relating to **[insert a brief, general description only where necessary and appropriate]**. **[Optional wording: We are addressing the matter through the appropriate procedures while respecting the privacy of those involved.]**

Everyone is entitled to express a view or raise a concern. However, we ask all members of our community to consider how online comments may be understood by others and the impact they may have on children, families and staff.

Online behaviour that threatens, intimidates, targets or humiliates another person may constitute bullying or harassment and, in some circumstances, may also raise safeguarding or potentially criminal concerns. Any concerns will be considered individually, fairly and in accordance with the relevant complaints, behaviour, safeguarding, staff conduct, health and safety or other appropriate procedures.

We ask parents and carers not to post or share content that may identify, target or cause harm to individual children, families or members of staff. This does not prevent anyone from raising a legitimate concern or making a complaint.

If you have a concern about **[school/setting name]**, please raise it directly with us so that we have an opportunity to understand and respond appropriately. Our complaints procedure and other relevant policies are available **[on our website at [link]/from the school or setting office]**.

Please continue to support us by:

- using the **[school/setting's]** agreed communication and complaints routes
- communicating respectfully, including when expressing disagreement
- considering the possible impact before posting or sharing content

- avoiding content that could identify or target children, families or staff
- modelling safe and responsible online behaviour for children

We value our relationship with parents and carers and want to work together to resolve concerns constructively and maintain a safe and respectful community.

If you would like to discuss this matter or have an online safety concern, please contact **[name and role/contact details]**.

Thank you for your support.

Yours sincerely

[Name]

[Headteacher/Manager/Chair of Governors or equivalent]

Letter to use with parents specifically involved in concerns

This template should be used with care and adapted to the circumstances. Wherever it is safe and appropriate, the setting should seek to discuss the concern with the parent or carer before sending a formal letter. Consider whether any safeguarding, police, HR or legal advice is required before making direct contact. A request to remove content or stop further posting should only be included where it is necessary and proportionate. The letter should not be used to discourage legitimate criticism, prevent a person raising a safeguarding concern or restrict access to the setting's complaints procedure.

Dear **[name of parent/carers]**

It has been brought to my attention that you have recently posted comments on **[site/platform]** relating to **[brief description of issue or event]**. I enclose a copy of the content that has been brought to the setting's attention so that we can discuss its context, your concerns and any appropriate next steps. *Any unrelated personal information should be removed from the copy provided, while an unaltered version should be retained securely where appropriate.*

I am concerned about the content and tone of the comments and their potential impact on members of our community. I would like to understand the concerns that led to the comments and discuss how these can be addressed through the appropriate channels. *Substitute for more appropriate adjectives if necessary.*

Where appropriate **[I ask that you do not post or share further comments about this matter while we are seeking to understand and address the concerns.]**

Where appropriate: [I ask that you remove the enclosed content because of its potential impact on [members of staff/children/other members of the community]. This request does not prevent you from raising your concerns through the setting's complaints procedure.]

Online behaviour that threatens, intimidates, targets or humiliates another person may constitute bullying or harassment and, in some circumstances, may also raise safeguarding or criminal concerns. We take concerns about possible bullying or harassment seriously and will consider each situation fairly and in accordance with the relevant procedures.

If you are dissatisfied with an aspect of the setting's work, you are encouraged to raise this through our complaints procedure, which is available [on our website/from the setting office/insert link or details]. This enables concerns to be considered properly and gives the setting an opportunity to respond.

Please contact me by [date or appropriate timeframe] to arrange a meeting so that we can discuss the matter openly and constructively. The discussion will be handled sensitively, and information will be shared only where necessary and appropriate.

Where appropriate: [My colleague [name and role] will be present to take a record of the meeting. You may also wish to be accompanied by a family member, friend or other appropriate person].

I hope that we can clarify the concerns and agree an appropriate way forward. If the matter cannot be resolved, or further concerns arise, the setting will review the situation and consider any additional action that may be appropriate in accordance with its policies.

I look forward to meeting with you.

Yours sincerely,
[Name]

[Headteacher/Manager/Chair of Governors or equivalent]

Disclaimer and Copyright

This guidance is based on original content developed by the [LADO Education Safeguarding Advisory Service](#), with input from the [Kent Area Directors for Education \(ADEs\)](#) and [Schools Personnel Service](#), and draws upon national advice and guidance from the [UK Safer Internet Centre](#).

Kent County Council makes every effort to ensure that the information in this document is accurate and up to date. If an error is brought to our attention, we will correct it as soon as reasonably practicable.

This guidance provides general information and should not be treated as a substitute for safeguarding, employment, police or legal advice about an individual situation.

Copyright in these materials is held by Kent County Council. Education settings are granted permission to reproduce and adapt all or part of the materials for their own not-for-profit purposes, provided that Kent County Council is acknowledged as the copyright holder and the materials are not sold, distributed commercially or presented as the intellectual property of another organisation.

Where settings adapt these materials for local use, they are responsible for ensuring that any amendments remain accurate, lawful and consistent with current national and local safeguarding guidance, procedures and arrangements.