ONLINE SAFETY POLICY

RESPONSIBILITIES	
To determine and approve policy and ensure compliance	ESA SLT
To implement, deliver and comply	Headteacher and SLT
APPROVAL DATE	February 2022
DURATION	2 Years
REVIEW DATE	February 2024
SLT LEAD	Headteacher

Contents

1. INTRODUCTION

Elstree Screen Arts recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all students, staff, governors and trustees will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of our students.

2. RESPONSIBILITIES

The Headteacher and Local Governing Body have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored in their school. All breaches of this policy must be reported to the school's e-safety coordinator.

All breaches of this policy that may have put a child at risk must also be reported to the school's Designated Safeguarding Person (DSP).

Organisations that are renting space from the school and are a totally separate organisation should have, and comply with, their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

3. SCOPE OF POLICY

The policy applies to:

- students
- parents/carers
- teaching and support staff
- school governors/trustees
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that students who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child to behave appropriately and keep themselves safe online.

This policy, supported by the acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other Trust and School policies and documents:

- Safeguarding and student welfare Trust)
- Child Protection and Training (Trust)
- Data Protection (Trust)
- Health and Safety Part I (Trust) and Part II (School)
- Home–school agreement (School)
- Behaviour (School)
- Anti-bullying (School)

4. POLICY AND PROCEDURE

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly in accordance with the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for students, parents/carers, staff, governors, trustees and all other visitors to the school.

Use of email

Staff, governors and trustees should use a school email account or Governor Hub for all official communication to ensure everyone is protected through the traceability of communications. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students may only use school approved accounts on the school system and only for educational purposes. Where required, parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection Policy. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors, trustees and students should not open emails or attachments from suspect sources and should report as soon as practicable to the school’s e-safety coordinator and ICT services team.

Users **must not** send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the e- safety coordinator with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online tools in order to communicate with students. When working with students, searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission is sought from the headteacher.

Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Students over the age of 13 can give their own consent. Records are kept on file and consent can be changed by parents/carers/students at any time (See privacy notices for greater clarification).

Photographs and images of students are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the headteacher. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly as appropriate.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons, parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than of their own child.

Staff and other professionals working with students, must only use school equipment to record images of students whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students. Under no circumstance does the school allow a member of staff to contact a student or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time at school events both on and off site, unless there is a pre- specified permission from the headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Students are allowed to bring personal mobile devices/phones to school but must not use them during the school day. All such devices must be switched off. Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

If staff personal mobiles are used to access school email and data they must be pin locked when not in use.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefits and carry out risk assessment before use in school is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL, the headteacher or the e-safety coordinator. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where appropriate, the DSL will refer details to social care services or the police.

5. CURRICULUM

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety that enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

6. STAFF AND GOVERNOR/TRUSTEE TRAINING

Staff, governors and trustees are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with students. (Appendix A)

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix E).

7. WORKING IN PARTNERSHIP WITH PARENTS/CARERS

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means. Students and parents are required to sign the Acceptable Use Agreement for students. (Appendix D)

8. RECORDS, MONITORING AND REVIEW

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors/trustees receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors/trustees ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. APPENDICES OF THE ONLINE SAFETY POLICY

A. Online Safety Acceptable Use Agreement – Staff, Governors, Trustees and student teachers (on placement or on staff)

B. Online Safety Acceptable Use Agreements Students

C. Online safety policy guide - Summary of key parent/carer responsibilities

D. Guidance on the process for responding to cyberbullying incidents

E. Guidance for staff on preventing and responding to negative comments on social media

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors, Trustees, visitors and student teachers

You must read this agreement in conjunction with the online safety policy and the Data Protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors/trustees are aware of their responsibilities in relation to their use. All staff and governors/trustees are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the e-safety coordinator. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the e-safety co-ordinator.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or students on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or students.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, trustees, parents/carers or students. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a student or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in Data Protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, students or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or GovernorHub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the GDPR. I will not use my school email addresses or GovernorHub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of students.

I will not access secure school information from personal devices unless a closed, monitorable system has been set up by the school.

External Hard drives and USB Sticks

The use of External Hard drives and USB Sticks is not allowed. Only school approved cloud storage or school network storage should be used.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the e-safety coordinator.

Promoting online safety

I understand that online safety is the responsibility of all staff, governors and trustees and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, trustees, visitors, students or parents/carers) to the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the e-safety coordinator

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor/trustee.

Signature ……………………………………………Date ……………………

Full Name (printed)

Job title ………………………………………………………………………

Appendix B - Online Safety Acceptable Use Agreement Students

- I will only use school IT equipment for school purposes.
- I will not download or install software on school IT equipment.
- I will only log on to the school network, other school systems and resources using my own school username and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will not use my personal email address or other personal accounts on school IT equipment.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal.
- If I accidentally come across any such material I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will immediately report any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- The use of External Hard drives and USB Sticks is not allowed. I understand that only school approved cloud storage or school network storage should be used.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- I will not attempt to bypass the internet filtering system in school.
- I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Student agreement

Student name…………………………………………………………………………

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Student signature………………………………………………………………………..

Date …………………………..

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Pupils are expected to read and discuss this agreement with you and then sign below to show they will follow the terms of the agreement. Any concerns or explanation can be discussed with the e-safety coordinator.

Please can you also sign and return the parent/carer agreement below. This document will be kept on

record at the school.

Pupil agreement

Pupil name…………………………………………………………………………

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature………………………………………………………………………..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……………………………………………………….

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.)

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/carer(s) signature(s) …………………………………….………………

Date ……………………………………………………………………

Appendix C - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for students.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that students can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable, block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix D - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Students should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix E - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide – Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a student are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

  The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings;
  - Ask for the offending remarks to be removed;
  - Explore the complainant's grievance;
  - Agree next steps;
  - Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

  - Reporting the matter to the social network site if it breaches their rules or breaks the law;

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to reiterate the seriousness of the matter.