



Policy Name:	Online Safety Policy
Owner:	Head of Pastoral /Director of IT
Named Governor with Lead Responsibility:	Dr Lumi Henshaw
Review Date: September 2025	Next Review date: September 2026
This Policy will be reviewed at least annually and revised as regulations or review demands.	

Contents:

1.	Policy Aims.....	2
2.	Policy Scope .....	2
3.	Monitoring and Review .....	3
4.	Roles and Responsibilities .....	3
4.1	The leadership and management team and governors will:.....	3
4.2	The Designated Safeguarding Lead (DSL) will: .....	4
4.3	It is the responsibility of all members of staff to:.....	4
4.4	It is the responsibility of the Director of IT to:.....	4
4.5	It is the responsibility of students (at a level that is appropriate to their individual age and ability) to: .....	5
4.6	It is the responsibility of parents, carers and guardians to: .....	5
5.	Education and Engagement Approaches.....	5
5.1	Education and engagement with students.....	5
5.2	Vulnerable Students .....	6
5.3	Training and engagement with staff .....	6
5.4	Awareness and engagement with parents and guardians. ....	6
6.	Responding to Online Safety Incidents and Concerns.....	6
6.1	Concerns about Students’ Welfare.....	7
6.2	Staff Misuse .....	7
7.	Procedures for Responding to Specific Online Incidents or Concerns .....	7
7.1	Child-on-child online sexual violence and sexual harassment .....	7
7.2	Youth Produced Sexual Imagery (‘Sharing nudes and semi nudes’) .....	8
7.3	Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines) .....	9
7.4	Indecent Images of Children (IIOC).....	9
7.5	Cyberbullying.....	10
7.6	Cybercrime .....	10
7.7	Online Hate .....	10
7.8	Online Radicalisation and Extremism .....	10
8	Safer Use of Technology .....	11
8.1	Classroom Use .....	11
8.2	Filtering and Monitoring.....	11
8.2.1	Decision Making .....	11
8.3.2	Filtering.....	11
8.3.3	Monitoring.....	12
8.4	Managing Personal Data Online.....	12
8.5	Security and Management of Information Systems.....	12
8.5.1	Password Policy .....	12
8.6	Managing the Safety of our Website. ....	13
8.7	Publishing Images and Videos Online.....	13
8.8	Managing Email .....	13
8.8.1	Staff Email .....	13
8.8.2	Student Email .....	13
8.9	Live Stream and Video Conferencing .....	13
8.10	Management of Learning Platforms .....	14
9	Social Media .....	14
9.1	Expectations .....	14

9.2 Staff Personal Use of Social Media .....	14
9.4 Students Use of Social Media.....	15
9.4 Official Use of Social Media.....	16
10 Use of Personal Devices and Mobile Phones .....	16
10.1 Expectations.....	17
10.2 Staff Use of Personal Devices and Mobile Phones .....	17
10.3 Students' Use of Devices and Mobile Phones .....	17
10.4 Visitors' Use of Personal Devices and Mobile Phones .....	18
10.5 School provided mobile phones and devices. ....	18
11 Useful Links.....	18

## 1. Policy Aims

This Online Safety Policy takes account of the DfE statutory guidance Keeping Children Safe in Education 2025 and the East Sussex Safeguarding Children Partnership procedures. The purpose of this Online Safety Policy is to:

- Safeguard and protect all members of our community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

We identify that the issues classified within online safety are considerable and ever evolving, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce/Contract:** risks such as online gambling, inappropriate advertising, phishing and or financial scams and sextortion (online sexual coercion and extortion of children).

## 2. Policy Scope

This Policy applies to all staff (including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the School) as well as students, parents and guardians. It also applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with School issued devices.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour e.g. online bullying or online safety incidents which may take place outside of the school but is linked to a member of the School. In this respect the School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/guardians of incidents of inappropriate online safety behaviour that has taken place out of School. Action can only be taken over issues covered by the published Behaviour Policy.

This Policy **links** with several other policies, practices and action plans including:

- Anti-bullying Policy;
- Acceptable Use Policies (AUP) and/or the Pupil Code of conduct;
- Behaviour Rewards Consequences and Pupil Voice Policy;
- Safeguarding and Child Protection Policy;

- Curriculum Policies, including Life Skills and Relationships and Sex Education (RSE);
- Data Protection Policy;

### **3. Monitoring and Review**

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. Our filtering system is tested monthly and test results recorded. To ensure they have oversight of online safety, the Head of Pastoral, Jodi Stone, will be informed of online safety concerns, as she holds overall lead responsibility for online safety.

The named Governor for Safeguarding, Dr Lumi Henshaw, will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

### **4. Roles and Responsibilities**

The Governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate safeguarding concerns when identified. The named governor Mr Andrew Larson is responsible for reporting to the governing body on a regular basis and meets regularly with the Director of IT, who is a member of the wider senior management team.

#### **4.1 The leadership and management team and governors will:**

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole School approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies (including the staff code of conduct and/or acceptable use policies) and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the School's IT system and therefore have appropriate filtering and monitoring systems in place, the effectiveness of which is regularly reviewed.
- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.
- Ensure that the DfE's filtering and monitoring standards for Schools and colleges are being met.
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all students to develop an age-appropriate understanding of online safety, tailored to the specific needs and vulnerabilities of individual children.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned, and considered as part of the whole School safeguarding approach and know how to escalate concerns when identified.
- Support the DSL and any deputies by ensuring they have the additional time, funding, training, resources and support they need to carry out the role effectively.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local, and national support.
- Audit and evaluate online safety practice, annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.

- Communicate with parents regarding the importance of children being safe online and the systems being used in School.

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

- Be an appropriate senior member of staff from the School Senior Leadership Team.
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs and the Director of IT, to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep students safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Along with the Director of IT, ensure that online safety is promoted to parents and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, through the MyConcern.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body.
- Work with the Senior Leadership Team to review and update online safety policies on a regular basis (at least annually) with stakeholder input, including from students.

#### **4.3 It is the responsibility of all members of staff to:**

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Read and adhere to the online safety policy and Acceptable Use Policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of electronic devices in lessons and other School activities
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reinforce the School's online safety messages when teaching lessons online.

#### **4.4 It is the responsibility of the Director of IT to:**

- Provide technical support and perspective to the DSL and wider Senior Management Team, especially in the development and implementation of appropriate online safety policies and procedures and compliance with DfE's filtering and monitoring standards for Schools and colleges.

- Implement appropriate security measures (including password complexity requirements, multi-factor authentication and deep packet inspection of internet traffic) to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Senior Management Team.
- Report any filtering breaches to the DSL (or deputy DSLs) and Senior Management Team.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

#### **4.5. It is the responsibility of students (at a level that is appropriate to their individual age and ability) to:**

- Engage in age-appropriate online safety education opportunities provided by the School.
- Read and adhere to Acceptable Use of ICT Policy (Pupil).
- Understand the importance of good online safety practice out of School and understand that this policy covers their actions outside of School if related to their membership of the School.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult or other support services, if there is a concern online, and support others that may be experiencing online safety issues.

#### **4.6 It is the responsibility of parents, carers and guardians to:**

- Encourage their children to adhere to the Acceptable Use Policy (Pupil).
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

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

### **5.1 Education and engagement with students**

- Mayfield School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at School and at home amongst students by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal Development, Life Skills, and Relationships and Sex Education (RSE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. This should include the use of generative AI tools and services.
  - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Mayfield School will support students to read and understand the Acceptable Use of ICT Policy (Pupil) in a way which suits their age and ability by:
  - Posting age-appropriate acceptable use posters on the Pupil Hub and signposting to this via Tutors.
  - Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation – emphasising that school managed devices are also monitored when not connected to the network.

- Rewarding positive use of technology and implementing appropriate peer education approaches.
- Seeking student voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

## **5.2 Vulnerable Students**

- We recognise that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO.

## **5.3 Training and engagement with staff**

Mayfield School will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff and governors on a regular basis, with at least annual updates. This training will take place during staff meetings, INSET days and as part of the reporting to Governor's cycle for Governors. This will cover the potential risks posed to students (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

## **5.4 Awareness and engagement with parents and guardians.**

- We recognise that parents and guardians have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats.
  - This will include offering specific online safety awareness training and highlighting online safety at other events.
  - Drawing their attention to the online safety policy and Acceptable Use of ICT Policy (Pupils) and expectations in newsletters, letters, our prospectus and on our website.
  - Providing them with information about our approach to filtering and monitoring.

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

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content and will be directed to the DSL in such circumstances.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- We require staff, parents, guardians and students to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, should be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the East Sussex Education Safeguarding Team.
- Where there is suspicion, that illegal activity has occurred contact the Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headmistress will contact Sussex Police first to ensure that potential investigations are not compromised.

### **6.1 Concerns about Students' Welfare**

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

### **6.2 Staff Misuse**

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

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

### **7.1 Child-on-child online sexual violence and sexual harassment**

Mayfield School has accessed and understood part 5 of Keeping Children Safe in Education September 2025.

- We recognise that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Personal Development, Life Skills and RSE curriculum.

- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
  - Immediately notify the DSL (or a deputy) and act in accordance with our child protection and anti-bullying policies.
  - If content is contained on students electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting, and removing online content, as well as providing appropriate counselling/pastoral support.
  - Implement appropriate consequences in accordance with our Behaviour Policy.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
  - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
  - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Sussex Police first to ensure that investigations are not compromised.
  - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

## **7.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')**

- We recognise youth produced sexual imagery as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or a deputy).
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS) document: Sharing nudes and semi-nudes: advice for education settings working with children and young people
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods through our personal development and RSE programmes.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.
- We will not:
  - View any images suspected of being youth produced sexual imagery, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented– in most cases, images or videos should not be viewed.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policy.
  - Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
  - Store the device securely. If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of students involved, including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Care and/or the Police, as appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate consequences in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the Senior Management Team will also review and update any management procedures, where necessary.

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

- We will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to students through a button on the pupil portal, so students can be empowered to report concerns.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant East Sussex Safeguarding Child Partnership's procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; Senior Management Team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If students at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

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

- We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) and we will seek to prevent accidental access to IIOC by using an appropriate filtering, firewalls, and anti-spam software.

- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.
- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy DSL) is informed, who will investigate the incident.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk) .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy DSL) and Headmistress are informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk) .
  - Ensure that any copies that exist of the image, for example in emails, are deleted once directed to by the police.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the Headmistress is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

### **7.5 Cyberbullying**

All staff will understand that children can abuse their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated here (see anti-bullying policy).

### **7.6 Cybercrime**

We will ensure that all members of the community are aware that children with skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.

### **7.7 Online Hate**

Online hate content, directed towards or posted by specific members of the community will not be tolerated at Mayfield School and will be responded to in line with existing policies, including anti-bullying and behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected.

### **7.8 Online Radicalisation and Extremism**

- Mayfield School will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation and we will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site. Our on-site internet connection is

filtered so that extremist material is blocked, and if any searches are made for extremist material, then these generate alerts (see monitoring and filtering section).

- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff or governor may be at risk of radicalisation online, the Headmistress will be informed immediately, and action will be taken in line with the child protection and allegations policies.

## 8 Safer Use of Technology

### 8.1 Classroom Use

- We use a wide range of technology. This includes access to:
  - Computers, laptops, tablets, phones, and other digital devices
  - Internet which may include search engines and educational websites.
  - Learning platforms
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras.
- All devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home.
- Mayfield School will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We suggest using Google as this is automatically safe search enabled when using School networked devices.
- We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- In the boarding environment, we will balance children's ability to take part in age-appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

### 8.2 Filtering and Monitoring

#### 8.2.1 Decision Making

- Our governors and senior leadership team have ensured that Mayfield School has age and ability appropriate filtering and monitoring in place on the internet connection provided by the school, to limit student's exposure to online risks, alongside effective classroom management and regular education about safe and responsible use.
- The governors and leaders have agreed that students can bring their own device to School to maximise their learning, although the school is moving towards a school-managed device from Sept 25, starting with students in Year 7. As part of the Pupil AUP, students using their own device on the school network are required to install anti-virus software.

#### 8.3.2 Filtering

- Mayfield broadband connectivity is provided through Coconnect and we use a Smoothwall firewall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) and Counter Terrorism Internet Referral Unit (CTIRU) lists.

- If a student finds a site that is blocked, that they wish to access for educational purposes, they should email the IT helpdesk, who will assess the site and if necessary consult with the DSL.

### **8.3.3 Monitoring**

- Mayfield monitors internet use on all school-managed devices and school internet connected personal devices which connect to the School infrastructure/network. This is achieved by using Senso Cloud to monitor school-managed devices and a Smoothwall Firewall which analyses traffic and generates alerts and reports based on activity.
- During Term time, if a safeguarding alert is triggered a notification will be automatically sent to the DSL, and the Head of Year/ School. Overnight the Boarding Housemistress will also be included. Concerns will be followed up as soon as is reasonable and parents will be contacted if there is a significant concern. During the School Holidays, if a safeguarding alert is triggered on a school-managed device, a notification will be sent to the DSL email, which is checked once a day Monday to Friday. Concerns will be followed up as soon as is reasonable and parents will be contacted in the event of a significant concern. Please be aware that safeguarding alerts cannot be triggered by student searches on personal devices not using the school network, so parents need to work in partnership with the school on responsibility for student online safety, especially in the holidays.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights, and privacy legislation.

## **8.4 Managing Personal Data Online**

Personal data will be recorded, processed, transferred, and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

## **8.5 Security and Management of Information Systems**

We adhere to and meet the DfE cybersecurity standards and take appropriate steps to ensure the security of our information systems, including:

- Protecting all devices on the School network with a properly configured boundary firewall and regularly updated virus protection.
- Keeping an up-to-date list of every device that can access the network and ensuring their security features are enabled, correctly configured and up to date.
- Ensuring that accounts only have the access that they require to perform their role and should be authenticated to access data and services.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- All users are expected to log off or lock their screens/devices if systems are unattended.

### **8.5.1 Password Policy**

- All members of staff and students will have their own unique username and passwords to access our systems. We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.
  - Use two-factor/two-step verification for all accounts which have access to personal or sensitive operational data and functions.

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

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) and we will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright. The administrator account for our website will be secured with an appropriately strong password.

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

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

### **8.8 Managing Email**

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately report offensive communication to the DSL and the Director of IT.

#### **8.8.1 Staff Email**

All members of staff are provided with a school email address to use for all official communication. The use of a personal email address by staff for any official business is not permitted. Staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students, and parents.

#### **8.8.2 Student Email**

Students will use provided email accounts for educational purposes. To use this they must sign the acceptable use policy and they will also will receive education regarding safe and appropriate email etiquette.

### **8.9 Live Stream and Video Conferencing**

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and students are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and students are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, students may be able to interact through a live chat function.
- When planning the use of live stream platforms teachers must ensure that student's behaviour/interactions are managed in line with the expectations of the School behaviour policy, Safeguarding Policy and the Blended and Remote Education Policy.
- Only live streaming platforms approved by SMT will be used. The platform of choice will be Microsoft Teams.

#### **8.9.1 Educational use of videoconferencing / live stream from other providers**

Staff directing students to any videoconferencing or live stream content from other providers, must check its suitability and appropriateness. Mayfield School recognises that video conferencing brings a wide range of benefits, but additional safety checks re suitability and appropriateness must be conducted, as our filtering and monitoring systems may not necessarily prevent inappropriate content from being shared in a live-streamed event as this is happening in real-time.

#### **8.9.2 Using video calls for 1:1 sessions with a student**

The School may consider using 1:1 video call sessions to support interventions and return to school transition. These sessions will only be provided where they have been approved by SMT and parental consent given. Any 1-1 online sessions will always be recorded. A copy of this recording will be available for 30 days. (See blended and remote learning policy for more information).

### **8.9.3 Online Tutoring**

Online Tutoring should complement the school's curriculum and support student learning goals—not supplant them. Therefore, tutoring must not take place during scheduled school lessons or activities and students may not miss school events for tutoring. See Online Tuition Policy Annex B of the Blended and Remote Education Policy for more information.

## **8.10 Management of Learning Platforms**

- Mayfield School uses Microsoft Teams and OneNote and all access and use takes place in accordance with our Acceptable Use Policies for Staff and Students. Only current members of staff, students will have access to the Teams. When staff /students leave school their account will be disabled.
- Students and staff will be advised about acceptable conduct and use when using Teams and One Note and all users will be mindful of copyright and will only upload appropriate content onto the platform.
- Any concerns about content on Teams and/or OneNote will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access for the user may be suspended and the user will need to discuss the issues with a member of leadership before reinstatement.
  - A student's parents may be informed.
  - If the content is illegal, we will respond in line with existing safeguarding procedures.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto a school team by a member of the leadership team as part of an agreed focus or for a limited time slot.

## **9 Social Media**

### **9.1 Expectations**

- The expectations' regarding safe and responsible use of social media applies to all members of Mayfield School community. This policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of our community are expected to engage in social media in a positive, safe, and responsible manner, and are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or that could damage the reputation of the School or individual within it.
- Concerns regarding the online conduct of any member of Mayfield School community on social media will be taken seriously and managed in accordance with the appropriate policies.

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

- Safe and professional online behaviour is outlined for all members of staff (including volunteers) as part of our Code of Conduct/ Staff behaviour policy as part of Acceptable Use of ICT Policy (Staff Annex A).
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated through training and the sharing of additional guidance and resources.

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school and staff are advised to safeguard themselves and their privacy when using social media sites. This may include (but is not limited to):
  - Setting the privacy levels of their personal accounts
  - Being aware of the implications of using location sharing services
  - Opting out of public listings on social networking sites
  - Logging out of accounts after use
  - Keeping passwords safe and confidential and using two factor authentication when available.
  - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Mayfield School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- Staff must exercise discretion when posting information and photographs on the internet. They should never refer to School matters on social networking or other internet sites, unless posting on official school accounts, or those with a professional focus, such as LinkedIn. School photographs should only be used with express permission. Information and content that staff members have access to as part of their employment, including information about students and their family members or colleagues should not be shared or discussed on personal social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

### **9.3 Communicating with students and their families**

- Staff should not give out any personal contact details to students or their family members. On School trips, staff should have a School mobile phone so they do not need to use their own device.
- Staff should not use any personal social media accounts to contact current students or their family members. If ongoing contact with students is required once they have left Mayfield, members of staff will be expected to use existing alumnae networks and/ or only use their school email address. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies).
- Members of staff who are 'friends' with parents should respect the advice contained in this policy and should, where reasonable, keep senior colleagues informed of any such relationships.
- Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).

### **9.4 Students Use of Social Media**

- Students in Year 7-11 should not use social media (or mobile phones more broadly) during the school day. Sixth Form students may use social media (or mobile phones more broadly) during school hours as long as they are in the Sixth Form centre and not attending lessons.
- As part of our curriculum, we help our students to acquire the knowledge to use social media in a safe, considered way and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, and as such we will not create or condone accounts for students under the required age.
- Any concerns regarding students' use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies, and shared with parents/ guardians as appropriate.
- Students will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/guardian or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords and two factor authentication where possible.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.
- To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

#### 9.4 Official Use of Social Media

Mayfield has set up official social media channels as distinct and dedicated social media sites for educational or engagement purposes. Staff must use a school provided email addresses to register for and manage any official social media channels and public communications on behalf of Mayfield. Mayfield School official social media channels are:

##### Instagram:

Mayfield School - [www.instagram.com/mayfieldSchool](http://www.instagram.com/mayfieldSchool)  
 Mayfield Sport - [www.instagram.com/mayfield\\_sport](http://www.instagram.com/mayfield_sport)  
 Mayfield Equestrian - [www.instagram.com/mayfield\\_equestrian](http://www.instagram.com/mayfield_equestrian)  
 Mayfield Food and Nutrition - [www.instagram.com/mgfoodandnut](http://www.instagram.com/mgfoodandnut)  
 Alumnae - [www.instagram.com/mayfieldschoolalumnae](http://www.instagram.com/mayfieldschoolalumnae)

##### Facebook:

School - [www.facebook.com/mayfieldgirls](http://www.facebook.com/mayfieldgirls)  
 Alumnae - [Old Cornelians | Facebook](#)

##### Twitter:

Mayfield School - @Mayfieldgirls  
 Mayfield Sport - @Mayfield\_Sport  
 Mayfield Library - @MGLibraries

##### LinkedIn

<https://www.linkedin.com/school/st-leonards-mayfield-school>

- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Always be professional and aware they are an ambassador for the Mayfield, although they should make it clear that they do not necessarily speak on behalf of the Mayfield.
  - Always be responsible, credible, fair, and honest, and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.
  - Before sharing pictures of students on social media, staff must check that parental permission has been obtained and that the pupils are not on the 'do not photo' list. Only the first name of girls should be used photos are captioned.

## 10 Use of Personal Devices and Mobile Phones

We recognise that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

### **10.1 Expectations**

- All use of personal electronic devices will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Behaviour, Child Protection and Staff Code of Conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user and all members of our community are advised to take steps to protect their devices from loss, theft, or damage. Mayfield School does not accept any responsibility for the loss, theft or damage of such items on our premises.
- The sending of abusive or inappropriate messages or content via personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour and safeguarding policies.
- All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

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

- Members of staff are advised to:
  - Keep mobile phones and personal devices in a safe place during lesson time and switched off or silenced.
  - Not use personal devices during teaching periods, unless permission has been given by the Headmistress such as in emergency circumstances.
  - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations. If a member of staff is thought to have illegal content saved or stored on a personal device or have committed a criminal offence, the police will be contacted.
- Members of staff are not permitted to use their own personal phones or devices for contacting students or parents and guardians. Any pre-existing relationships, which could undermine this, will be discussed with the Headmistress or DSL (or deputies).
- Staff must not use a personal device to take photos or videos of students and will only use School provided equipment for this purpose.

### **10.3 Students' Use of Devices and Mobile Phones**

- During the school day, mobile phones must be handed in by girls in Years 7 – 11. Year 12 and 13 are only to use mobile phones in the Sixth Form centre. Anyone not adhering to this will have their mobile phone confiscated until the end of the school day.
- Public areas, such as the Hub, Dining rooms, corridors and Year 7-11 common rooms are all designated 'screen-free' zones. Girls should not be using laptops or tablets for any purpose (including academic work) in these areas.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity or lesson, it will only take place when approved by the Senior Management Team.
- Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- If a student in Year 7 – 11 needs to contact their parents/guardians whilst on site, they may use their own phone under supervision or use a school phone, for example at reception
- If a student requires access to a personal device in exceptional circumstances, for example medical assistance this will be discussed with a staff member prior to use being permitted.

- Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy and in line with the DfE searching, screening and confiscation guidance.
- Students' mobile phones or devices may be searched by a member of the Senior Management Team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted if it contravenes our policies.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

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

Visitor (including parents, volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use. Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headmistress of any breaches our policy.

#### 10.5 School provided mobile phones and devices.

- Members of staff will be issued with a work phone number where regular contact with students, parents and guardians is required. School mobiles and devices will be suitably protected via a passcode and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.
- Staff will not use WhatsApp to communicate with students who are under the age of 13.

### 11 Useful Links

#### Links for Schools

- UK Council for Internet Safety (UKCIS): [www.gov.uk/government/organisations/uk-council-for-internet-safety](http://www.gov.uk/government/organisations/uk-council-for-internet-safety)
- UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
- SWGfL: 360 Safe Self-Review tool for schools [www.360safe.org.uk](http://www.360safe.org.uk)
- Childnet: [www.childnet.com](http://www.childnet.com)
- Step Up Speak Up – Online Sexual Harassment Guidance: [www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals](http://www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals)
- Cyberbullying Guidance: [www.childnet.com/resources/cyberbullying-guidance-for-schools](http://www.childnet.com/resources/cyberbullying-guidance-for-schools)
- PSHE Association: [www.pshe-association.org.uk](http://www.pshe-association.org.uk)
- National Education Network (NEN): [www.nen.gov.uk](http://www.nen.gov.uk)
- National Cyber Security Centre (NCSC): [www.ncsc.gov.uk](http://www.ncsc.gov.uk)
- Educate against hate: <https://educateagainsthate.com>
- NCA-CEOP Education Resources: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- Safer Recruitment Consortium: [www.saferrecruitmentconsortium.org/](http://www.saferrecruitmentconsortium.org/)
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)
- Project Evolve: <https://projectevolve.co.uk>
- Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
- Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
- NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)

#### Reporting Helplines

- NCA-CEOP Safety Centre: [www.ceop.police.uk/Safety-Centre](http://www.ceop.police.uk/Safety-Centre)
- Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

- ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
- Report Remove Tool for nude images: [www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online](http://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety sexting/report-nude-image-online)
- Stop it now! [www.stopitnow.org.uk](http://www.stopitnow.org.uk)
- The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
- Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)
- Report Harmful Content: <https://reportharmfulcontent.com>
- Revenge Porn Helpline: <https://revengepornhelpline.org.uk>
- Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)

#### **Support for children and parents/carers**

- Childnet: [www.childnet.com](http://www.childnet.com)
- Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
- Parent Zone: <https://parentzone.org.uk>
- NSPCC: [www.nspcc.org.uk/online-safety](http://www.nspcc.org.uk/online-safety)
- Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
- Parents Protect: [www.parentsprotect.co.uk](http://www.parentsprotect.co.uk)
- Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org)
- NCA-CEOP Child and Parent Resources: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)