Mobile Phone, Smart Technology & Online Safety Policy

Camp Beaumont | Camp Beaumont ASIA | In2 action | In2assessments

Mobile Phone, Smart Technology & Online Safety (e-safety) Policy

Policy Purpose & Aims

This policy outlines the appropriate use of mobile phones, smart technology, and communication devices by staff, visitors, and children to maintain safeguarding, privacy, and professionalism across all Camp Beaumont sites. This policy aims to promote online safety, safeguard and protect all members of the Camp Beaumont Group community online.

Roles and Responsibilities

Camp Beaumont Group Safeguarding Leads
Camp Beaumont Group has designated the Chief Executive Officer for Camp Beaumont UK & Asia and the Executive Director for In2action as the Safeguarding Leads with organisational responsibility for Safeguarding with their individual purview. This responsibility is inclusive of the setting the framework around the Group's Mobile Phone, Smart Technology & Online Safety (e-safety) Policy.

Operational & DSL Responsibility
The Operational, Training & Recruitment Teams and Designated Safeguarding Leads are responsible for ensuring this policy is trained, understood and each member of staff has the resource to execute the policy in full. Maintain records of mobile phone, smart technology and online safety concerns to inform the Safeguarding Advisory Group (SAG) of trends as well as keeping up to date on current research, legislation and guidance that could improve our approach to safeguarding.

Camp Management & OSL Responsibility
The Camp Management Team and Onsite Safeguarding Leads are responsible for ensuring compliance with this policy among all staff members. Act as a named point of contact for any safeguarding issues relating to mobile phones, smart technology and online safety.

Staff Responsibility
All members of the Camp Beaumont Group have the responsibility to ensure they and others follow this policy across all undertakings, promote online safety and ensure all the children and adults are safeguarded from harm.

Non-Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action in accordance with Camp Beaumont's code of conduct and safeguarding procedures. Repeated or serious breaches may lead to further investigation or termination of employment.

Liability

Camp Beaumont does **not** accept responsibility for loss or damage to any personal belongings, including smart watches, brought on-site by staff or management.

Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Safeguarding Policy
- Code of Conduct
- Operations Manual
- Prevent Policy
- Confidentiality Policy
- Data Protection Act 2018
- General Data Protection Regulations
- Data (Use and Access) Act 2025
- Sexual Offences Act 2003
- Human Rights Act 1998

Monitoring and Review

- Camp Beaumont Safeguarding Advisory Group (SAG) will review this policy annually.
- The policy will also be revised following any national or local policy requirements, any child or adult protection concerns, or any changes to the technical infrastructure.
- We will continue to apply restrictions to the material users' access.
- To ensure they have oversight of online safety, the Safeguarding Lead will be informed of online safety concerns, as appropriate.
- The named Safeguarding Lead will report on a regular basis to the SAG on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the SAG's action planning.

Mobile Phone Use

Staff Mobile Phones (Camp Beaumont UK & Asia)
Personal mobile phones are **not permitted** for use under any circumstances while staff are fulfilling their duties, other than for staff members to clock-in and clock-out of their shift. Staff may bring personal phones when arriving for duties but must store them securely in their bags, which are left in the camp office or staff room if available. Camp offices are either occupied by management or securely locked. Staff who drive to work may choose to leave their phones in their locked vehicles.

Personal Phone Procedure
Before starting each shift, staff must leave their phone in a designated child free area, for example camp office or staff room. During breaks, staff may access their phones **only** in designated **child-free areas** (e.g., staff room or off-site). Upon resuming duties, staff must ensure their phone has been securely stored again.

Camp Beaumont UK & Asia Issued Mobile Phones
Each site is issued with a camp mobile phone for operational use. This number is provided to parents via booking confirmations, on the website, and displayed at the entrance of each camp. Only the camp management team is authorised to use this phone for inbound and outbound calls and messages. The Camp Beaumont central team (Operations, Operations Coordinators, Customer Service, Marketing) will contact camps only during operational hours using this designated number.

Children's Mobile Phones (Camp Beaumont UK & Asia)
Parents are informed via the **Parent Welcome/Information Pack** that children are **not permitted** to bring mobile phones to camp. If a child is seen using a mobile phone during the day, it will be **confiscated** and returned at the end of the day. Camp Beaumont is **not responsible** for any mobile phones brought to camp by children.

For Camp Beaumont Asia residential camps, children may bring a mobile phone or other electronic devices. All devices will be signed in on arrival and stored securely. Devices will only be returned to children during designated access times, with all use monitored through a mobile/electronic device sign-in and sign-out log.

Visitor Mobile Phones
All external visitors must **turn off** their mobile phones and leave them in their bag or a designated secure place at the camp for the duration of their visit. Members of the central Camp Beaumont Group team must remain contactable for operational purposes. They may keep **work phones** on but must take/make calls **away from children**. Central team members must **not** carry personal phones while on-site.

Smart Technology Use

Smart Watches:
Camp Beaumont acknowledges that staff may wear smart watches for various reasons.
However, the following rules apply:
Smart watches with independent camera capabilities must be treated the same as mobile phones and follow the procedures outlined above.

Usage Expectations

- **Professional Boundaries:** Smart watches must not interfere with staff's ability to supervise or engage with children. Personal use should be limited to breaks or non-contact periods.
- **Notifications:** All notifications should be **disabled** during working hours to minimize distractions unless **explicitly approved** by management.
- **Professionalism:** Smart watches should not be used in ways that may appear unprofessional or inattentive, especially during activities, meetings, or interactions with children and parents.

Privacy and Safeguarding

- **Recording Restrictions:** The use of smart watches for **recording audio, taking photos, or capturing videos** is strictly prohibited in areas where children are present.
- **Child Interaction:** Children must **never** be allowed to use or interact with staff members' smart watches, including playing games, sending messages, or viewing media.
- **Health Exceptions:** Staff with medical conditions requiring monitoring via smart watch (e.g., heart rate, glucose levels) must **inform management**. Reasonable accommodations will be made to support health needs while maintaining safeguarding standards.

On-site Communication

Use of Two-Way Radios
Access to a radio will be provided to camp management teams and all activity groups. Alternatives may be used on a case by case basis which will be determined by a local risk assessment.

Radio Usage Guidelines
Radios must be carried by authorised staff **at all times** during sessions, except during breaks. Each group must have **at least one radio** to ensure they can contact the management team or request assistance if needed. Radios should be used **professionally and responsibly** to ensure clear and efficient communication across the camp.

Online Safety (e-safety)

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices.

Types of online risk usually fall under one of three categories:

- **Contact:** Contact from someone online who may wish to bully or abuse the child or adult. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting personal information.
- **Content:** Inappropriate material available to children or adults online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.
- **Conduct:** The child or adult may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Defining online abuse

"Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones" (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- Harassment
- Stalking
- Threatening behaviour
- Creating or sharing child sexual abuse material
- Inciting a child to sexual activity

- Sexual exploitation
- Grooming
- Sexual communication with a child
- Causing a child to view images or watch videos of sexual act

Education and Engagement Approaches

Camp Beaumont will establish and embed a progressive E-Safety awareness raising programme throughout Camp Beaumont sites, to raise awareness and promote safe and responsible internet use amongst all by:

- Ensuring awareness regarding safe and responsible use precedes internet access.
- Reinforcing online safety messages across Camp Beaumont sites including use of Camp Beaumont systems and personal technology.

Camp Beaumont will support all in reading and understanding the Code of Conduct and AUP in a way which suits their age and ability by:

- Displaying acceptable use posters across each Camp Beaumont site.
- Informing all that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Seeking visitor feedback regarding Camp Beaumont E-safety to support the future development of online safety policies and practices.
- Using support, such as external visitors, where appropriate, to complement and support the Camp Beaumont internal online safety awareness approaches.

Vulnerable Individuals

- Camp Beaumont is aware that some individuals are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with SEND or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss together with adults at risk for similar circumstances.
- Camp Beaumont will ensure that differentiated and ability appropriate online safety awareness, access and support is provided to those individuals (which is age appropriate).

Training and engagement with staff

Camp Beaumont will:

- Provide and discuss the Mobile Phone, Smart Technology & Online Safety (e-safety) Policy with all staff as part of their induction.
- Provide up-to-date and appropriate online safety training for all staff.
- Continue to remind and educate staff to behave professionally and in accordance with Camp Beaumont policies when accessing Camp Beaumont systems and devices.
- Make staff aware that their online conduct out of Camp Beaumont, including personal use of social media, could have an impact on their professional role and reputation with Camp Beaumont.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting children, young people, adults at risk, colleagues or other members of the Camp Beaumont community.

Awareness and engagement with parents, carers and group leaders

Camp Beaumont recognises that parents, carers and group leaders supporting individuals attending Camp Beaumont have an essential role to play in enabling them to become safe and responsible users of the internet and associated technologies.

Camp Beaumont will build a partnership approach to online safety:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the Camp Beaumont Mobile Phone, Smart Technology & Online Safety (e-safety) and Code of Conduct and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of attending Camp Beaumont.

Reducing Online Risks

Camp Beaumont recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a Camp Beaumont computer or device.

All members of the Camp Beaumont community are made aware of the Camp Beaumont expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the Camp Beaumont Code of Conduct and highlighted through a variety of awareness raising approaches.

Safer Use of Technology

Educational Use

Camp Beaumont uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Camp Beaumont platforms
- Emails
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

All Camp Beaumont owned devices will be used in accordance with IT AUP and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in any setting. Camp Beaumont will ensure that the use of internet derived materials, by staff and visitors, complies with copyright law and acknowledges the source of information.

Supervision of children, young people and adults at risk will be appropriate to their age and vulnerability.

Managing Internet Access

- Camp Beaumont will maintain a written record of users who are granted access to Camp Beaumont devices and systems.
  - For our camp venues, the camp management teams are the only people who are granted access to Camp Beaumont systems.
  - For our central (head) office, all employees are provided with access to Camp Beaumont systems as part of their role. All access is subject to role-based permissions, password controls, and monitoring in line with our GDPR, Data Protection, and Information Security policies.
- All staff, and visitors will read and sign Code of Conduct/AUP before being given access to the Camp Beaumont computer system, IT resources or internet.

Filtering and Monitoring

Decision Making

- Camp Beaumont SAG have ensured that appropriate filtering and monitoring is in place, to limit exposure to online risks.
- Camp Beaumont decision regarding filtering and monitoring have been informed by a risk assessment.
- Changes to the filtering and monitoring approach will be risk assessed by staff with technical experience and, where appropriate, with consent from the SAG; all changes to the filtering policy are logged and recorded.
- SAG will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard; effective management and regular awareness raising about safe and responsible use is essential.

Filtering

- Camp Beaumont uses broadband connectivity via their Internet Service Provider.
- Camp Beaumont uses appropriate filtering systems which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- Camp Beaumont filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Camp Beaumont works with its Internet Service Provider/Filtering Provider to ensure that our filtering policy is continually reviewed.

Dealing with Filtering Breaches

Camp Beaumont has a clear procedure for reporting filtering breaches.

Step 1
If individuals discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediately to a member of staff.
Step 2
The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead.
Step 3
The breach will be recorded and escalated as appropriate.
Step 4
Parents/carers will be informed of filtering breaches involving their child/ adult.
Step 5
Any material that Camp Beaumont believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Police.

Monitoring

- Camp Beaumont will appropriately monitor internet use on all Camp Beaumont owned or provided internet enabled devices.
- Camp Beaumont has a clear procedure for responding to concerns identified via monitoring approaches.
- All users will be informed that use of Camp Beaumont systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Security and Management of Information Systems

Camp Beaumont takes appropriate steps to ensure the security of our information systems.

- Virus protection is being updated regularly.
- 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.
- Regularly checking files held on the Camp Beaumont network,
- The appropriate use of user logins and passwords to access the Camp Beaumont network. (Specific user logins and passwords will be enforced for all).
- All users are expected to log off or lock their screens/ devices if systems are unattended.

Password policy

All members of staff will have their own unique username and private passwords to access Camp Beaumont. Members of staff are responsible for keeping their passwords private.

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.

Managing the Safety of the Camp Beaumont Website

- Camp Beaumont will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) and in line with OFSTED.
- Camp Beaumont will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- No personal information will be published on our website; the contact details on the website will be the Camp Beaumont address, email and telephone number.
- The administrator account for the Camp Beaumont website will be secured with an appropriately strong password.
- Camp Beaumont will post appropriate information about safeguarding, including online safety, on the Camp Beaumont website for members of the community.

Managing Email

Access to Camp Beaumont email systems will always take place in accordance with Data Protection legislation and in line with other Camp Beaumont policies, including: confidentiality and the Code of conduct.

- 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.
- Camp Beaumont email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the Camp Beaumont community will immediately inform the DSL if they receive offensive communications, and this will be recorded in the Patronus.

Staff

The use of personal email addresses by staff for any official Camp Beaumont business is not permitted except where required for business communications, and an official Camp Beaumont email address was not provided.
All members of staff are provided with a specific Camp Beaumont email address, to use for all official communication.

Use of Video conferencing and/or Webcams

Camp Beaumont recognises that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.

- All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto answer.
- Videoconferencing contact details will not be posted publicly.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

- Camp Beaumont staff or responsible individuals, consent will be obtained prior to any child, young person or adult at risk taking part in videoconferencing activities.
- Videoconferencing will be supervised appropriately, according to age and ability.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.

- The unique login and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

- When recording a videoconference, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, Camp Beaumont will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- Camp Beaumont will establish dialogue with other conference participants before taking part in a videoconference; staff will check that the material they are delivering is appropriate for the class.

Social Media

The expectations regarding safe and responsible use of social media applies to all members of Camp Beaumont community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.

All members of the Camp Beaumont community are expected to engage in social media in a positive, safe, and responsible manner at all times.

All members of the Camp Beaumont community 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.

Camp Beaumont will control access to social media whilst using Camp Beaumont provided devices and systems on site.

Inappropriate or excessive use of social media during work hours or whilst using Camp Beaumont devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of Camp Beaumont community on social media, should be reported to the DSL and will be managed in accordance with our Anti-bullying, Allegations against staff, Code of conduct and Safeguarding policies.

Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Camp Beaumont Code of conduct.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within Camp Beaumont. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include but is not limited to:

- Setting the privacy levels of their personal sites as strictly as they can.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as those of Camp Beaumont.

Members of staff are encouraged not to identify themselves as employees of Camp Beaumont on their personal social networking accounts. This is to prevent information on these sites from being linked with Camp Beaumont and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with Camp Beaumont policies and the wider professional and legal framework.
Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.

Members of staff will notify the DSL immediately if they consider that any content shared on social media sites conflicts with their role in Camp Beaumont.

Communicating with visitors and party leaders

All members of staff are advised not to communicate with or add as 'friends' any current or past guests, or current or past guest's family members via any personal social media sites, applications or profiles.

- Any preexisting relationships or exceptions that may compromise this will be discussed with the DSL.
- If ongoing contact with guests is required once they have concluded their time at Camp Beaumont, members of staff will be expected to use existing corporate networks and official Camp Beaumont provided communication tools.

Staff will not use personal social media accounts to make contact with guests or parents, nor should any contact be accepted. Any communication from guests and parents received on personal social media accounts will be reported to Camp Beaumont DSL.

Guests' Personal Use of Social Media

Any concerns regarding children, young people or adults at risk use of social media, whilst with Camp Beaumont, will be dealt with in accordance with existing policies including Anti-bullying policy. Concerns will also be raised with parents, as appropriate, particularly when concerning underage use of social media sites or tools.

E-safety advice for guests will include:

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/protected.

- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within Camp Beaumont and externally.

Official Use of Social Media

Camp Beaumont has a range of official social media channels.

The official use of social media sites, by Camp Beaumont, only takes place with clear educational or community engagement objectives, with specific intended outcomes.

- The official use of social media as a communication tool has been formally risk assessed and approved by SAG.

Official Camp Beaumont social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

- Staff use Camp Beaumont provided email addresses to register for and manage any official Camp Beaumont social media channels.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from the Camp Beaumont website.
- Public communications on behalf of Camp Beaumont will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality, Code of Conduct, Social Media Guidelines and Safeguarding procedures.

- All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents and guests will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Parents and carers will be informed of any official social media use with guests, and written parental consent will be obtained through our child information questions as part of the booking process.

Staff expectations

Members of staff who follow and/or like the Camp Beaumont social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of Camp Beaumont, they will:

- Sign the Camp Beaumont social media Acceptable use policy.
- Be professional at all times and aware that they are an ambassador for the organisation.
- Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of Camp Beaumont.
- Be responsible, credible, fair and honest at all times 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.
- Ensure that they have appropriate written consent before posting images on the official social media channel.

- Not disclose information, make commitments or engage in activities on behalf of Camp Beaumont unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, guests, parents and carers.
- Inform their Designated Safeguarding Lead of any concerns, such as criticism, inappropriate content or contact from guests.

Responding to Online Safety Incidents and Concerns

All members of the Camp Beaumont community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery, cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official Camp Beaumont procedures for reporting concerns.

- Pupils, parents and staff will be informed of Camp Beaumont complaints procedure and staff will be made aware of the whistleblowing procedure.
- Camp Beaumont requires staff, parents, carers and guests to work in partnership to resolve online safety issues.
- After any enquiries are completed, Camp Beaumont will debrief, identify lessons learnt and implement any policy.
- If Camp Beaumont is unsure how to proceed with an incident or concern, the DSL will seek advice from the Multi Agency Safeguarding Hub (MASH).
- Where there is suspicion that illegal activity has taken place, Camp Beaumont will contact the MASH/ 101, or 999 if there is immediate danger or risk of harm.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding, child or adult protection concerns.
- The DSL will record these issues in line with Camp Beaumont policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Board thresholds and procedures.
- Camp Beaumont or the relevant group will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to Designated Safeguarding Lead according to the Safeguarding policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

- Camp Beaumont recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- Camp Beaumont will follow the advice as set out in national guidance.
- Camp Beaumont will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches. Camp Beaumont will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'Sexting'

If Camp Beaumont are made aware of an incident involving the creation or distribution of youth produced sexual imagery, they will:

Step 1
Act in accordance with safeguarding policies and manual of operations and the relevant Local Safeguarding Children's Board procedures.

Step 2
Immediately notify the Designated Safeguarding Lead

Step 3
Store the device securely. If an indecent image has been taken or shared on the Camp Beaumont network or devices, Camp Beaumont will take action to block access to all users and isolate the image.

Step 4
Carry out a risk assessment which considers any vulnerability of children, young people and adults at risk involved; including carrying out relevant checks with other agencies.

Step 5
Inform parents and carers, if appropriate, about the incident and how it is being managed.

Step 6
Make a referral to children's social care, MASH and/or the Police, as appropriate.

Step 7
Provide the necessary safeguards and support for children, young people, and adults at risk, such as offering counselling or pastoral support.

Step 8
Images will only be deleted once Camp Beaumont 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.

Step 9
Review the handling of any incidents to ensure that best practice was implemented; the SAG will also review and update any management procedures, where necessary.

Camp Beaumont will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off Camp Beaumont premises, using Camp Beaumont or personal equipment.

Camp Beaumont will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. (In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented on Patronus).
- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request guests to do so.

Online Child Sexual Abuse and Exploitation

Camp Beaumont will ensure that all members of staff 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.

Camp Beaumont recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

Camp Beaumont will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate methods of communication for guests and parents.

Camp Beaumont will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

Dealing with Online Child Sexual Abuse and Exploitation

If Camp Beaumont is made aware of an incident involving online sexual abuse of a child, young person or adult at risk, they will follow protocol as detailed in the sexting guidelines.

If Camp Beaumont is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the MASH and/or respective regional Police.

If Camp Beaumont is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the MASH and respective Police by the DSL.

If individuals outside Camp Beaumont are believed to have been targeted also, Camp Beaumont will seek the support from Police and/or MASH first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

Camp Beaumont will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

Camp Beaumont will take action regarding IIOC on their equipment and/or personal equipment, even if access took place off site.

Camp Beaumont will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If Camp Beaumont is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through their local Police and/or MASH.

If made aware of IIOC, Camp Beaumont will:

- Act in accordance with the Camp Beaumont Safeguarding policy and operational manual and the relevant local Safeguarding Child Board procedures.
- Immediately notify the DSL.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), MASH/ Police and or the LADO.

If made aware that a member of staff, child, young person or adult at risk has been inadvertently exposed to indecent images of children whilst using the internet, Camp Beaumont will:

- Ensure that the Designated Safeguard Lead is informed.

- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via 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 Camp Beaumont devices, they will:

- Ensure that the DSL is informed.
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Identify where all copies of the images are held.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social care (as appropriate) - **UK only**.
- Inform the police or safeguarding agency of the country where the incident has occurred using the details found in the Safeguarding Policy appendices – **Asia only**.
- 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 Camp Beaumont devices, Camp Beaumont will:

- Ensure that the DSL is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with Camp Beaumont allegations procedures – **UK only**.
- Report using the guidelines in accordance with the country where the incident took place – **Asia only**.
- Quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Camp Beaumont. Full details of how Camp Beaumont will respond to cyberbullying are set out in the Anti-bullying policy and Code of conduct.

Online Hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at Camp Beaumont and will be responded to in line with existing Camp Beaumont policies, including Anti-bullying and Code of Conduct.

All members of the community will be advised to report online hate in accordance with relevant Camp Beaumont policies and procedures. The Police will be contacted if a criminal offence is suspected.

If Camp Beaumont is unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the MASH and/or local Police as identified in Local Arrangements Documents. Camp Beaumont Asia will contact their local police or safeguarding agency accordingly.

Online Radicalisation and Extremism

Camp Beaumont will take all reasonable precautions to ensure that children, young people and adults at risk are safe from terrorist and extremist material when accessing the internet through Camp Beaumont systems.

If anyone is concerned that a child, young person or adult at risk or any other member of the Camp Beaumont Community may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with Camp Beaumont Safeguarding/Prevent policies.

See also Camp Beaumont Prevent policy and Safeguarding manual.