Camp – Online Safety Policy

Version number	1.1
Consultation groups	Central Executive Team, DPO, Extended Services team
Approved by	Board of Trustees
Approval date	23 March 2023
Adopted by	Advisory Board
Adopted date	May 2023
Policy/document owner	Trust Online Safety Lead
Status	Statutory
Frequency of review	2 Years
Next review date	March 2024
Applicable to	Discovery Trust Holiday Camps

Document History

Version	Version Date	Author	Summary of Changes
V1.0	9th September 2021	Adam Lapidge – Online Safety Lead	*New policy prepared in line with:* ▪ *Keeping children safe in education -September 2021* ▪ *Working Together to Safeguard Children", 2018* ▪ *Ofsteds Review of Sexual Abuse and Colleges – June 2021*
V1.1	May 2023	Adam Lapidge DPO, Louise Barber and Jo Venables	*Reviewed and ammeded for Holiday Camps*

Contents

1. Statement of Intent

The online safety policy is intended to demonstrate the organisation's commitment to:

- Ensuring the safety and wellbeing of children, young people and adults is paramount when using the internet, social media or mobile devices.
- Providing staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensuring that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all Holiday Camp members, including staff, children, volunteers, parents, carers, visitors, and community users who have access to and are users of Trust digital technology systems, both in and out of the Trust.

2. Linked policies

This policy statement should be read alongside our organisational policies and procedures, including:

- Acceptable Use policy (KS1 & KS2)
- Anti-Bullying Policy (including Cyberbullying)
- Document Retention Management Policy
- GDPR Data Protection Strategy
- Mental Health and Wellbeing Policy
- Mobile Phone and Smart technology policy
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Pupil Behaviour Policy
- Social Media Policy
- Special Educational Needs and Disability Policy
- Home Learning Protocol Policy

Staff related Policies and Procedures:

- Acceptable Use policy
- Disciplinary Policy and Procedure
- Mobile Phone and Loaned Property Policy
- Staff handbook which includes Staff Code of Conduct
- Staff Wellbeing Policy
- Trust Platform Working document

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for online safety.

- **3. Key Roles and Responsibilities**

The school takes a whole-school approach to online safety and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all staff and volunteers read and understand this policy and implement it consistently.

3.1 Trust Online Safety Lead

The role of Online Safety lead forms part of the Trust's safeguarding team. The Trust Online Safety Lead will receive regular training on online safety and be aware of the potential for serious child protection and/or safeguarding issues that may arise from the online world. They will have overall oversight of the trust's online safety strategy. Key responsibilities:

- Deliver training to the Extended Services Manager to ensure they are up to date with the latest online safety issues.
- Ensuring support mechanisms are in place for Holiday Camps for dealing with complex situations.
- Ensuring that there are robust protocols in place for both monitoring and reporting online safety issues.
- Responsible for actioning the annual review of the online safety policy.

3.2 Head Teachers/Head of Schools and SLT

Head teachers / Head of school take overall responsibility in ensuring that all staff and children understand and follow the policies and procedures of online safety.

Key responsibilities:

- Support the Extended Services Manager in carrying out their role within their school setting.
- To know the procedures in the event of serious online safety allegations against a member of staff.
- Reviews the school's infrastructure/network with the Director of IT or Senior Technician to ensure it is safe and fit for purpose.

3.3 Extended Services Manager

The Extended Services Manager has overall responsibility for ensuring that staff and children who are attending Holiday Camps are following the procedures and policies set out for online safety.

Key Responsibilities:

- Ensuring that all employed staff are given training as part of their induction.
- Ensure that all employed staff read, review, and accept the Online Safety Policy and any other related documents (Acceptable Use Policy etc).

- Ensure they are clear on the procedures in the event of a serious online safety allegation against a member of staff.
- Have clear policies and procedures around the use of digital technology at Holiday Camps.

3.4 School IT Technicians

School IT technicians are the first line of defense against online safety, and they play a huge role in ensuring that pupils and staff are kept safe. Key responsibilities are to:

- Ensure that school networks are secure and safe to use.
- Regularly monitor school networks and internet.
- implement and update monitoring software/systems are as requested by Trust's senior technical team.
- Ensure that only authorised users can access the network and these users adhere to the trust's password policy.
- Ensure that filtering policies are applied to the correct users.
- Ensure that any filtering request changes are liaised and agreed with the Extended Services Manager before actioning.
- Ensure that any online safety incidents are sent the Extended Services Manager so that they can be actioned.

3.5 Children

Children are responsible for:

- Ensuring that they use the digital technology systems in accordance with the pupil acceptable use policy.
- Understanding the importance of reporting abuse, misuse, or access to inappropriate material.
- Adhering to the school mobile phone policies and are aware of the consequences if they don't follow this.
- Understanding the need for good online safety behaviour both in and out of school.
- Providing valuable feedback about online safety through surveys and discussions.

4. Online safety concerns

4.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

4.2 Peer on peer abuse

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

The school will respond to all concerns regarding online peer-on-peer sexual abuse and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

4.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Pupils are less likely to report grooming behaviour because:

- The pupil believes they are talking to another child
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

4.4 Child sexual exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CSE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

4.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

4.6 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

Where there are any concerns about a pupil's use of technology and their intentions about using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

- **5. Responding to online incidents**
- **5.1 Responding to pupil incidents.**

When a child misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The Extended Services Manager will determine the seriousness of all incidents and report all illegal activities/incidents to the appropriate organisation, these include:

- Police
- CEOP (child exploitation and online protection)

- **5.2 Responding to staff incidents.**

Where a staff member misuses the school's IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

- **6. Personal devices**

6.1 Children

Children attending holiday camps may bring mobile devices into school. Parents/Carers will need to complete an agreement that their child can bring a mobile phone into school because the child will be walking themselves to or from camp, or for another reason as determined appropriate. Children must hand their mobile device to the Site Leader who will ensure it is kept securely. Children are not allowed to use their mobile phone during the camp day.

Any breach of the mobile device agreement may trigger disciplinary action in line with the behaviour policy and could result in confiscation of their device.

6.2 Staff

Whilst at work, staff members must not use a personal device (e.g., phones and tablets), unless this is in their break/lunch time and in a room not used by children. Staff are not permitted to take or store images of pupils on their mobile device. Personal information about staff, pupils, or the school is not to be stored on any personal device.

Personal mobile phones must not be used to contact pupils or parents. During school outings nominated staff will have access to a school mobile phone which can be used for emergencies or contact purposes.

- **7. Policy review**

This policy will be reviewed by the Trust Online Safety Lead annually and updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. A formal review will be completed every two years for Trust Board approval.