THE RANCH
Weymouth
@theranchweymouth

Online Safety Policy Statement 2024 - 2025

Monitored by the Board of Directors:

Iain Woodbridge IainWoodbridge
Toni Matthews Toni
James Matthews Woodbridge JamesMW
Diana Glencross Diana

Statement of Intent

The Ranch Weymouth understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. It is important that The Ranch Weymouth therefore have a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

● **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

● **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

● **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

● **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk.

Our provision has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

Ethos: The Ranch Weymouth works with children and families as part of its activities. These include: Providing Alternative Education Provision, Animal Assisted Interventions and education re-engagement.

Children and young people should never experience abuse of any kind. Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

The purpose of this policy is to:

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

Scope and Limitations

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

As an education setting we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. We want to ensure that the whole Ranch community – pupils, parents, carers and staff – are responsible users and stay safe when using the internet and other technologies for educational, personal and recreational use.

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

This policy has been written with the support of:
nspcc.org.uk/learning
learning@nspcc.org.uk

Individuals named in this Policy:

Overview by Iain Woodbridge Designated Safeguarding Lead (Level 3)
Ann-Marie Carter Deputy Designated Safeguarding Lead (Level 3) and Administration Lead
Toni Matthews (RGN) Director and Lead Facilitator (Safeguarding Level 2)
in conjunction with Sarah Stilwell Operational System Administration (Safeguarding Level 2)
Sheryl Dyer (RGN) Education Lead
Shannon Furze Designated LAC Key Worker

Related policies and procedures

This policy operates in conjunction with the following policies and procedures of The Ranch Weymouth: All of which can be found on our public website. www.theranchweymouth.com

Social Media Policy

Allegations of Abuse

Cyber-security Policy

Cyber Response and Recovery Plan

Safeguarding and Child Protection Policy

Anti-Bullying Policy

Staff Code of Conduct

Behaviour Policy

Disciplinary Policy and Procedure

Data Protection Policy

Mobile Phone and Devices Policy

Camera, Observation and Photography Procedure

Definitions

DSL - Designated SafeGuarding Lead
DDSL - Deputy Designated Lead
LA - Local Authority
ASDAN - is an education charity and awarding organisation providing courses, accredited curriculum programmes and regulated qualifications.
PSHE - Personal, social, health and economic education
SEND - Special educational needs and disabilities
LAC - Looked After Child

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

● Voyeurism (Offences) Act 2019

● The UK General Data Protection Regulation (UK GDPR)

● Data Protection Act 2018

● DfE (2021) 'Harmful online challenges and online hoaxes'

● DfE (2023) 'Keeping children safe in education 2023'

● DfE (2023) 'Teaching online safety in school'

● DfE (2022) 'Searching, screening and confiscation'

● Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

● UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

● National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

2. Roles and responsibilities

The board of Directors will be responsible for:

● Ensuring that this policy is effective and complies with relevant laws and statutory guidance.

● Ensuring the DSL's remit covers online safety.

● Reviewing this policy on an annual basis.

● Ensuring their own knowledge of online safety issues is up-to-date.

● Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

● Ensuring that there are appropriate monitoring systems in place.

● Ensuring that all staff have an awareness and understanding of contextual Safeguarding and know how to escalate concerns when identified.

● Ensuring that all the relevant policies of The Ranch Weymouth have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Director and Lead Facilitator Toni Matthews, will be responsible for:

● Ensuring that online safety is a running and interrelated theme throughout The Ranch's policies and procedures, including in those related to staff training and safeguarding.

● Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

Working with youth support staff and the administration team to document children and young people who attend the setting have a named keyworker to raise concerns, this will then be entered on the register with the child's name.

Work with the youth support staff and named key workers of the pupils to ensure that pupils have awareness and knowledge of who the designated safeguarding lead and deputy designated safeguarding lead are. This information is communicated visually on displayed posters and via regular news feeds on Class Dojo.

Supporting the youth support staff and the Education Lead Sheryl Dyer that the young people and children that attend The Ranch Weymouth have online safety sessions within the ASDAN PSHE learning framework and via The Ranch Weymouth internet work booklet and displayed posters.

● Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.

● Ensuring online safety practices are audited and evaluated; by way of monthly supervisions and appraisals, reflective practice, taking place overseen by the DSL and head of staffing.

● Organising engagement with parents to keep them up-to-date with current online safety issues and how The Ranch is keeping pupils safe. Including but not limited to; newsletters, ClassDojo engagement and face to face feedback. Including but not limited to: Parents/carers are kept up to date on any legislative changes that impact The Ranch

Weymouth's policies via Class Dojo, email mail, newsletters. All policies and procedures are also accessible on The Ranch Weymouth's public domain website.

● Working with the DSL and Operational systems administrator Sarah Stilwell to conduct termly light-touch reviews of this policy.

● Working with the DSL and the board of Directors to update this policy on an annual basis.

Auditing at least termly the permissions as submitted by parents/carers, remain relevant and up to date. This will be done by assigning the Administration Lead and DDSL to send out pupil information and data capture form to parents/carers via email invitation. This ensures that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given. This permission is entered on the register entry and central data for the individual pupil; any limitations marked in red. On The Ranch Weymouth SharePoint MicroSoft 365.

The DSL will be responsible for:

● Taking the lead responsibility for online safety in the setting.

● Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

● Liaising with relevant members of staff on online safety matters, e.g. youth key workers, the operational systems administrator.

● Ensuring online safety is recognised as part of The Ranch's safeguarding responsibilities and that a coordinated approach is implemented.

● Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of The Ranch community understand this procedure. This is via the Incident Report Form and or Safeguarding Concern Report Form hosted on The Ranch Weymouth Microsoft SharePoint 365.

● Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

● Monitoring online safety incidents to identify trends and any gaps in The Ranch's provision, and using this data to update The Ranch's procedures.

● Reporting to the board of Directors about online safety on a termly basis.

● Working with the Lead Facilitator and Operational systems administrator, to conduct termly light-touch reviews of this policy.

● Working with the Lead facilitator and board of Directors to update this policy on an annual basis.

Operational Systems Administrator will be responsible for:

● Providing technical support in the development and implementation of The Ranch's online safety policies and procedures.

● Implementing appropriate security measures as directed by the DSL and Lead Facilitator.

● Working with the DSL and Lead Facilitator to conduct termly light-touch reviews of this policy.

Working with the Administration Lead, as part of our registration procedure and document capture, parents are asked to provide informed consent and agreement to how images of their child is used, including but not limited to uploading of digital images. This is then noted next to the main register database and all staff with access to The Ranch Weymouth's social media is informed.

Education Lead will be responsible for:

Taking responsibility and working to support the youth support staff to deliver to the young people and children that attend The Ranch Weymouth have online safety sessions within the ASDAN PSHE learning

framework and via The Ranch Weymouth internet work booklet and displayed posters.

All staff members will be responsible for:

● Taking responsibility for the security of ICT systems and electronic data they use or have access to.

● Modelling good online behaviours.

● Maintaining a professional level of conduct in their personal use of technology.

● Having an awareness of online safety issues.

● Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.

● Reporting concerns in line with The Ranch's reporting procedure.

● Where relevant to their role, ensuring online safety is embedded in their youth support work with individuals.

Promoting and displaying child centred support signposts to services such as 'Report Remove Tool', NSPCC, The Ranch 'Safeguard Superheroes' posters.

Children and young people who attend the setting will also have a named keyworker to raise concerns alongside knowledge of who the designated safeguarding lead and deputy designated safeguarding lead are. This information is communicated visually on displayed posters and via regular news feeds on Class Dojo.

The young people and children that attend The Ranch Weymouth have online safety sessions within the ASDAN PSHE learning framework and via The Ranch Weymouth internet work booklet and displayed posters.

Pupils will be responsible for:

● Seeking help from The Ranch team members if they are concerned about something they or a peer have experienced online.

● Reporting online safety incidents and concerns in line with the procedures within this policy.

Role of Parents/carers and pupils

All members of The Ranch Weymouth community – pupils, parents, staff and visitors , are asked to sign and return an Acceptable Use Agreement to ensure everyone understands how digital and information technologies can be used safely, in and out of school.
Any concerns regarding online safety should be reported to the named keyworker, DSL or youth support team, initially who will pass this on to the safeguarding lead if necessary.

For more information on safer ways to use the internet please click below:

http://www.saferinternet.org.uk
Safer Internet Day 2021 films
http://parentzone.org.uk
https://www.thinkuknow.co.uk
Tik Tok – what parents need to know

Here's a link to a lesson on the BBC all about staying safe online:

https://www.bbc.co.uk/teach/live-lessons/safer-internet-day-live-lesson/zdh2wnb

At the time of registering a placement with The Ranch Weymouth parents/carers are provided with an agreement to sign. Parents/carers are asked to read and discuss this agreement as outlined below, with their child and then sign it.

Young person's agreement
I will be responsible for my behaviour when using the internet, including social media

platforms, games and apps. This includes the resources I access and the language I use.
I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately and seek support from my key worker.
I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
I will not give out any personal information online, such as my name, phone number or address.
I will not reveal my passwords to anyone.
I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or group leader and am accompanied by a trusted adult.
If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to my key worker or Woody (Iain Woodbridge) and Ann-Marie Carter.
I understand that my internet use on devices owned by The Ranch Weymouth will be monitored and logged. I understand that these rules are designed to keep me safe and that if I choose not to follow them, The Ranch Weymouth may contact my parents/carers.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for The Ranch's approach to online safety, with support from deputies and the lead facilitator where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour. If the pupils involved are registered as a dual roll placement, the DSL will contact the named school's DSL by phone and email as soon as practically possible to communicate information.

The importance of online safety is integrated across all The Ranch's operations in the following ways:

● Staff and the board of Directors receive annual training

● Staff receive regular updates regarding online safety information and any changes to online safety guidance or legislation. They are aware of reporting and next steps. This awareness is clarified at monthly supervisions and appraisals and monthly reflective practice.

● Parents are sent termly information about being safe online through the ClassDojo system.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress. If the child is registered as a dual roll placement, the DSL will contact the named school's DSL as soon as practically possible by phone and email.

All concerns are recorded in an individual Safeguarding Concerns folder on The Ranch Weymouth's Safeguarding Hub hosted on SharePoint MicroSoft 365.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the DSL, who decides on the best course of action in line with the relevant policies. If the concern is about the DSL, it is reported to the Deputy DSL and Lead Facilitator, who will seek guidance from CHAD on how to proceed.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Lead Facilitator and operational systems administrator, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the DSL contacts the police.

The Ranch Weymouth avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and The Ranch Weymouth's response are recorded by the DSL on the secure Safeguarding hub hosted The Ranch Microsoft Sharepoint 365.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

● Threatening, intimidating or upsetting text messages

● Threatening or embarrassing pictures and video clips sent via mobile phone cameras

● Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible

● Threatening or bullying emails, possibly sent using a pseudonym or someone else's name

● Unpleasant messages sent via instant messaging

● Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

● Abuse between young people in intimate relationships online i.e. teenage relationship abuse

● Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The Ranch Weymouth will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of The Ranch setting, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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

● Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless.

Youth Support Staff will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The Ranch will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The Ranch Weymouth will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The Ranch Weymouth will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the setting premises. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

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 and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. 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.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

● Being secretive about how they are spending their time online.

● Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

● Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Youth Support Staff will having ongoing training and youth work courses that aid them in the awareness of the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Youth Support Staff will be able to provide session interventions in balance to support the understanding of pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.around the subject of;

● Boundaries in friendships with peers, in families, and with others

● Key indicators of grooming behaviour

● The importance of disengaging from contact with suspected grooming and telling a trusted adult

● How and where to report grooming both in The Ranch setting and to the police.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

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.

CCE 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.

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.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Safeguarding and Child Protection Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. All staff have mandatory PREVENT training, this training is held on their staff file and training matrix and updated regularly. Staff files are hosted on the central Staffing and HR Management of The Ranch Sharepoint Microsoft 365.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Safeguarding and Child Protection Policy.

7. Mental health

Staff will be aware that online activity both in and outside of The Ranch setting can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in The Ranch community, they will report this to the DSL

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to The Ranch setting or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Lead Facilitator will decide whether each proposed response is:

● In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.

● Careful to avoid needlessly scaring or distressing pupils.

● Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.

● Proportional to the actual or perceived risk.

● Helpful to the pupils who are, or are perceived to be, at risk.

● Appropriate for the relevant pupils' age and developmental stage.

● Supportive.

● In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and lead facilitator will only implement a Ranchl-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. 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 Ranch Weymouth 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 with regard to 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.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities of them as youth support workers. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and mentoring

Education Lead will be responsible for:

Taking responsibility and working to support the youth support staff to deliver to the young people and children that attend The Ranch Weymouth have online safety sessions within the ASDAN PSHE and Citizenship learning framework and via The Ranch Weymouth internet work booklet and displayed posters.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

● How to evaluate what they see online

● How to recognise techniques used for persuasion

● Acceptable and unacceptable online behaviour

● How to identify online risks

● How and when to seek support

● Knowledge and behaviours that are covered in the government's online media literacy strategy

The DSL will be involved with the development of The Ranch's online safety lesson planning. Pupils will be consulted on the online safety lesson planning, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the named key worker and designated key worker for LAC, Iain Woodbridge and Shannon Furze will work together to ensure the lesson planning is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The Ranch Weymouth will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Youth Support Staff will review external resources prior to using them to ensure they are appropriate for their assigned pupils.

External visitors may be invited into The Ranch setting to help with the delivery of certain aspects of the online safety. The Lead Facilitator and DSL will decide when it is appropriate to invite external groups into the setting and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the key worker/youth support staff and DSL will consider the topic that is being covered and the potential that pupils have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the youth support staff/key worker will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology while at The Ranch setting.

A range of technology will be used during sessions, including the following:

- Laptops

- Tablets - iPads

Prior to using any websites, tools, apps or other online platforms, or recommending that pupils use these platforms at home, the youth support staff will review and evaluate the resource.

Pupils will be supervised when using online materials during session time – this supervision is suitable to their age and ability.

13. Use of smart technology

While The Ranch recognises that the use of smart technology can have emotional regulation benefits, there are also a variety of associated risks which The Ranch will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices.

Staff will use all smart technology and personal technology in line with The Ranch's Electronic Devices Policy and Staff Conduct Policy.

The Ranch recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches The Ranch's ethos and Behaviour Policy.

Inappropriate use of smart technology may include:

● Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.

● Sharing indecent images, both consensually and non-consensually.

● Viewing and sharing pornography and other harmful content.

Pupils will be governed by The Mobile Phone Policy and those that breach the expected behaviours, where it is deemed necessary will not be permitted to use smart devices or any other personal technology whilst in The Ranch setting.

The Ranch will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The Ranch will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The Ranch Weymouth will work in partnership with parents to ensure pupils stay safe online at the setting and at home. Parents will be provided with information about The Ranch's approach to online safety and their role in protecting their children. Parents are encouraged to go through ClassDojo communications with their child to ensure their child understands..

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

● Child sexual abuse, including grooming.

● Exposure to radicalising content.

● Sharing of indecent imagery of pupils, e.g. sexting.

● Cyberbullying.

● Exposure to age-inappropriate content, e.g. pornography.

● Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

● ClassDojo

Email Communications

● Team Around the Family Meetings

● Online resources

15. Internet access

Pupils, staff and other members of The Ranch community will only be granted access to The Ranch's internet network by use of a temporary password. A record will be kept of users who have been granted internet access in the offsite and onsite office.

16. Monitoring online activity

If staff while using devices provided by The Ranch, such as tablet, laptop access material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the DSL who will contact the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The Ranch owned devices will be appropriately monitored. All users of The Ranch Wifi and The Ranch owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network Security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the operational systems administrator. Firewalls will be switched on at all times. The operational systems administrator will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the operational system administrator and inform the DSL.

All members of staff will have their own unique usernames and private passwords to access The Ranch's systems. Staff members will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 90 days, after which users will be required to change them.

Users will inform the operational systems administrator if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the head of staffing will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Full details of The Ranch's network security measures can be found in the Cyber-security Policy.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Staff will be given approved The Ranch Weymouth email accounts and will only be able to use these accounts at The Ranch and when doing The Ranch-related work outside of setting hours. Prior to being authorised to use the email system, staff must have had induction training and pass all relevant security DBS checks. Personal email accounts will not be permitted to be used on The Ranch site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to the operational systems administrator. The Ranch Weymouth uses the onboarding Microsoft 365 monitoring system which can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

The Lead facilitator and the operational systems administrator retain oversight of all emails provided to The Ranch staff. All emails are viewable from the central administration panel hosted by Microsoft 365.

19. Generative artificial intelligence (AI)

The Ranch Weymouth do not use AI in any sessions or ASDAN projects.

20. Social networking

The use of social media by staff will be managed in line with The Ranch's Social Media Policy and Staff Conduct Policy.

21. The Ranch website

The Lead Facilitator will be responsible for the overall content of The Ranch Weymouth website – they will ensure the content is appropriate, accurate, up-to-date.

22. Use of devices

The use of personal devices on The Ranch premises and for the purposes of related work will be managed in line with the Staff Electronic Devices Policy and Staff Code of Conduct.

As The Ranch staff access the secure data via their personal devices, they will be responsible to implement and manage a firewall to protect any data accessed for work purposes. The files are hosted securely and centrally by Microsoft 365 and One Drive, and must be accessed via The Ranch SharePoint 365; each step requires the staff to input a password. Protections are onboard to protect the data via the Microsoft software.

The Ranch will be aware that security standards may change over time with changing cyber threats. The Ranch will ensure that the security of every device that has been provided by The Ranch is reviewed regularly. Staff members and team members that use their own personal devices will be responsible for the security of the data from The Ranch is reviewed regularly.
The Ranch will require authentication for users to access sensitive data.

To ensure that The Ranch data is as secure as possible, all staff and team members have the responsibility to:
• Avoid leaving devices with access to The Ranch data in unlocked or unattended locations.
• Change default device passwords.
• Immediately change passwords which have been compromised or suspected of compromise. Immediately inform the DSL and the operational systems administrator.

23. Monitoring and review

The Ranch Weymouth recognises that the online world is constantly changing; therefore, the DSL, operational systems administrator and the Lead Facilitator will conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The board of Directors, Lead Facilitator and DSL will review this policy in full on an annual basis and following any online safety incidents.

We are committed to reviewing our policy and good practice annually. This policy was last reviewed on:

March 2024 - The next scheduled review date for this policy is **March 2025.**

Any changes made to this policy are communicated to all members of The Ranch Weymouth community.

Signed by The Board of Directors:

Iain Woodbridge, Toni Matthews, James Matthews Woodbridge, Diana Glencross

Appendices

List of terms and concerns:

Disinformation, Misinformation and hoaxes:

Some information shared online is accidentally or intentionally wrong, misleading or exaggerated.

Online hoaxes: which can be deliberately and inadvertently spread for a variety of reasons ●

The widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online

Fake websites and scam emails: Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain.

Online fraud: Fraud can take place online and can have serious consequences for individuals and organisations. Online fraud can be highly sophisticated and that anyone can be a victim

Children are sometimes targeted to access adults' data.

Password phishing: Password phishing is the process by which people try to find out individuals' passwords so they can access protected content.

Personal data Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'.

Persuasive design: Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.

Privacy settings: Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Privacy settings have limitations.

Targeting of online content: Much of the information seen online is a result of some form of targeting. Adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts. The concept of clickbait and how companies can use it to draw people to their sites and services.

Online abuse: Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. ● The types of online abuse, including sexual harassment, bullying, trolling and intimidation ●

Radicalisation: Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals.

Challenges: Online challenges acquire mass followings and encourage others to take part in what they suggest. Challenges which include threats or secrecy, such as 'chain letter' style challenges.

Content which incites violence: Knowing that violence can be incited online and escalate very quickly into offline violence. Online content (sometimes gang related) can glamorise the possession of weapons and drugs. To intentionally encourage or assist in an offence is also a criminal offence.

Fake profiles: Not everyone online is who they say they are. In some cases, profiles may be people posing as someone they are not or may be 'bots'.

Unsafe communication: Communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with.

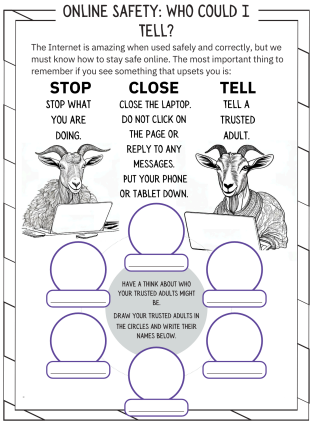
Wellbeing Impact on quality of life, physical and mental health and relationships: When online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Pupils should consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out.

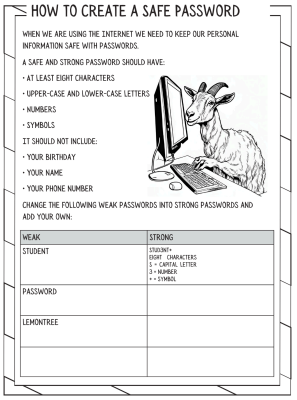
Excessive social media usage can have on levels of anxiety, depression and other mental health issues.

Online vs. offline behaviours: People can often behave differently online to how they would act face to face. People can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure. People are unkind or hurtful online when they would not necessarily be unkind to someone face to face.

Suicide, self-harm and eating disorders: Pupils may raise topics including eating disorders, self-harm and suicide.

Example of The Ranch Weymouth safe internet usage workbook:





Example of The Ranch Weymouth Safeguard Poster: