THE RANCH
Weymouth
@theranchweymouth

Cyber Security Policy

March 2024
To be Reviewed Spring 2025

The Board of Directors:

Iain Woodbridge woody@theranchweymouth.com
Toni Matthews toni@theranchweymouth.com
James Matthews Woodbridge james@theranchweymouth.com
Diana Glencross

The Ranch Weymouth recognises that Cyber Security is an essential function to protect not only our own Company's assets and functions, but also to safeguard and protect the sensitive data we may hold and process about the young people and children under our educational care.

This Policy should be read together with:
Child Protection & Safeguarding
Online Safety & Agreement
GDPR & Data Protection
Staff Code of Conduct
These Policies may be found on our public domain website or by following the above hyperlinks
www.theranchweymouth.com
The statutory guidance which schools and colleges must comply with is Keeping Children Safe in Education 2023
It contains information on what schools and colleges should do and sets out the legal duties with which schools and colleges must comply and should be read alongside Working Together to Safeguard Children 2023.

Useful Contacts:
The Regional Cybercrime lead is ACC Julie Fielding.
Dorset Police's Strategic Lead is Detective Chief Superintendent Mark Cooper.
Detective Sergeant Tim Farrell is the contact for Dorset Police's Dedicated Cybercrime unit
Cybercrime Prevention Officer is Jake Moore

Pan-Dorset Multi-Agency Safeguarding Procedures
Safeguarding and Standards Team on 01305 221122 or email
SafeguardingAndStandardsAdvisors@dorsetcouncil.gov.uk

Cyber security is the process by which individuals and organisations reduce the risk of a cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information stored on these devices, and online.

The Ranch Weymouth is aware of the growth of Cyber Crime activities and has procedures and processes in place to minimise both the opportunities for an attack taking place, and to minimise any resulting damage arising out of a malicious attack.

We take the potential threat of Cyber Attack seriously, and all staff must abide by this policy, and its associated policies, including:

- Clear Desk and Screen Policy
- E-Safety
- GDPR Policy
- Social Media Policy
- Social Networking Guide for Staff
- Staff Acceptable Use of Technology Declaration

Current Cyber Security Threats

A Cyber Threat Actor (CTA) is a participant (person or group) in an action or process that is characterized by malice or hostile action, using computers, devices, systems, or networks. CTAs are classified into groups based on their motivations and affiliations and include:

- **Cybercriminals** - profit-driven and represent a long-term, global, and common threat. They target data to sell, hold for ransom, or otherwise exploit for monetary gain.
- **Insiders** - current or former employees, contractors, or other partners who have access to an organisation's networks, systems, or data. Malicious insiders intentionally misuse their access in a manner that negatively affects the confidentiality, integrity, or availability of the organisation's information or information systems. This is distinct and separate from employees who unintentionally cause damage to their organisation's information systems through their actions, such as clicking on malicious links in a phishing email, which is the number one cause of cyber-attacks.
- **Foreign Government** - aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.
- **Hacktivists** (Ideologically-Motivated Criminal Hackers) are politically, socially, or ideologically motivated and target victims for publicity or to effect change.
- **Terrorist Organisations** – activity is typically disruptive or harassing in nature.

Types of Cyber-Attack

Common types of cyber-attack include:

- **Malware** - Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:
  - o Block access to key components of the network (ransomware)
  - o Installs malware or additional harmful software
  - o Covertly obtains information by transmitting data from the hard drive (spyware)
  - o Disrupt certain components and renders the system inoperable
- **Phishing** - Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine.

Phishing is an increasingly common cyberthreat. A Cyber attack made via text message or SMS is known as Smishing.

- **Man-in-the-middle attack** - Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. Two common points of entry for MitM attacks are:
  - o 1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
  - o 2. Once malware has breached a device, an attacker can install software to process all of the victim's information.
- **Denial-of-service attack** - A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.
- **SQL Injection** - A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- **Zero-day exploit** - A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

Phishing (and Smishing)

Whilst cyber-attacks can come in many forms, the number one cause of cyber security breaches is Phishing or Multi-Layered Phishing (Social Engineering).

Phishing emails are designed to trick an individual into divulging sensitive information or will include a malicious link or attachment which if clicked on or opened will download Malware on to your computer and/or network.

Whilst some Phishing emails may contain obvious spelling or grammar mistakes, Cyber Criminals are becoming more sophisticated and may include personal information to give their appearance validity.

Phishing emails will often include 'urgency' and 'authority' cues to pressure you to act quickly and without thinking, for example, your payment has been declined, 'click here to avoid further action', or claim to be from a person in authority, for example a CEO.

The Ranch Weymouth's employees are expected to be familiar with the organisation's policies and procedures and to double check the validity of an email or instruction if something seems unusual. This checking must not be undertaken by responding to the email rather they should telephone a trusted contact.

'Phishers' will use publicly available information to make their emails more convincing so employees should consider reviewing privacy settings on social media settings.

Employees are not permitted to post online about The Ranch and/or The Ranch's clients or organisational activity which is not already in the public domain or provided or approved by The Ranch Weymouth.

Spotting scam emails is tricky, but things to look out for include:

- official-sounding messages about ‘resetting passwords’, ‘receiving compensation’, ‘scanning devices’ or ‘missed deliveries’;
- emails full of ‘tech speak’, designed to sound more convincing; • being urged to act immediately or within a limited timeframe. The message will often claim to be from an authority figure (like a bank, or power company).
- Remember, your bank (or any other official organisation) will **never** ask you to supply personal information.

If you have any doubts:

- contact the organisation directly using their official website or social media channels. Don’t use the links or contact details in any messages you have been sent.
- Hover over the recipient to see the full originating email address; an email address can be set to appear as something like “Lloyds Bank” in the settings, but if you hover over this name, it could be from ‘clicktogetphished@scammer.com’.
- If a suspicious email arrives which appears to be from someone within your organisation, call them to check.

The Designated Safeguarding Lead Iain Woodbridge (Level 3), the Deputy Designated Safeguarding Lead Ann-Marie Carter (Level 3) in conjunction with the IT System and Operational Administrator Sarah Stilwell and supported by the board of directors will help your staff to spot unusual requests

This will be through monthly supervisions with Iain Woodbridge to explore the staff members understanding and through ongoing internet safety training delivered by newsletters, email, staff meetings and Sharepoint 365 communications.

This will be by communicating questions such as:
Do colleagues and staff at your school know what to do with unusual emails or phone calls, and where to get help?

Ask yourself whether someone impersonating an important individual (a parent, manager, or member of the local authority) would be challenged by everyone in The Ranch Weymouth.

Think about how you can encourage and support your staff to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask ‘is this genuine?’ can be the difference between staying safe, or a costly mishap.

Implications of a Cyber Attack

Disruption of Academic Activities: A cyber attack at The Ranch Weymouth may lead to significant disruption in the delivery of education. The Ranch Weymouth's digital infrastructure may be rendered inoperable, affecting communication channels, timetables, and access to crucial learning resources. Students and staff would face challenges in continuing their academic activities, causing a loss of valuable instructional time and productivity.

Privacy and Data Breach Concerns: The breach of sensitive student data and administrative records raises serious concerns about privacy and data protection. Personal information, including names, addresses, and contact details, may be compromised, potentially exposing students and staff to various risks such as identity theft and targeted scams

Reputational Damage: The cyber attack would inflict reputational damage on The Ranch Weymouth, eroding the trust and confidence of students, parents, and the wider community. A breach would highlight any vulnerability to cyber threats and raise questions about The Ranch Weymouth's ability to safeguard critical data and ensure a secure learning environment. Rebuilding trust and reputation in the aftermath of such an incident requires substantial efforts and long-term cybersecurity investments.

Cyber Security Measures

The Ranch Weymouth has the following protective measures in place to minimise the risk of a cyber-attack:

- Firewalls installed at all sites with wifi access.
- Anti-virus installed on all sites
- Automatic patch updates (to ensure security updates are installed without delay) • Ransomware protection running on all devices supplied by subscription to Microsoft Office 365.
- Spam filtering through the use of staff work email addresses which are filtered through the security systems inbuilt into Microsoft defender enhanced Outlook mail.
- Office365 (includes Multi Factor Authentication Capabilities)
- Secure document sharing and storage – Sharepoint
- System for the updating of passwords and removal of access when an employee leaves our employment
- Regular Reviews of Live Report Scheduling Service
- Websites built with protection from Wix security and SSL certificates for all sites, plus automated vulnerability scans regularly conducted.
- Limitation of, and removal of unnecessary email addresses.

User Information and Education

The Ranch Weymouth advocates a User Information and Education approach to Cyber Security in addition to the measures outlined in this policy, and ensures all relevant users have access to training courses to support this.

This will be delivered via the sharepoint 365 training library and displayed in staff areas.

Reporting Culture & Processes

The Ranch Weymouth understand that a reporting culture in which errors are identified and reported as soon as possible can minimise the impact of any potential breach and highlight areas for additional training and/or improvement in our processes. Any employee who believes they have accidentally clicked on a suspicious link, opened a malicious attachment or in any other way potentially breached or allowed the breach of our internal systems, must report this immediately to both our Designated Safeguarding Lead Iain Woodbridge woody@theranchweymouth.com or if not available the Deputy Designated Safeguarding Lead Ann-Marie Carter office@theranchweymouth.com and to the System Operations Administrator Sarah Stilwell sarah@theranchweymouth.com .

If a member of staff receives a suspicious email, and have not been able to check it's validity with a trusted contact within the organisation, or they have confirmed it has not originated from them, this must be reported internally using the same process as above, and also to the Suspicious Emails Reporting Service (SERS) on report@phishing.gov.uk

Suspicious SMS should be reported internally, as above, and also by forwarding the SMS to 7726 (remember 'SPAM' on a telephone keypad). Please note you will be asked to provide the telephone number you have received the suspicious SMS from so do not delete the message before you have completed the reporting process.

If you've been tricked into providing your banking details, contact your bank and let them know.

If you've given out your password, you should change the **passwords** on any of your accounts which use the same password.

Incidents of fraud and cybercrime will be reported to Action Fraud.

Cyber Security and Data Breaches

A cyber security breach may also represent a personal data breach (or put the The Ranch Weymouth or its clients at risk of one). It is therefore essential that if you believe a cyber breach may have taken place, you report this immediately to the DDL so a decision can be taken as to whether the breach is reportable to the Information Commissioner's Office.

Third Party Applications

As part of its day to day operations, The Ranch Weymouth and employees use a number of third party applications, including the below. These third party applications have their own systems for ensuring the security of the data including but not limited to:

- Local Authority Reporting/Disclosure barring service and other secure systems
- Sage
- SharePoint 365
- Government Gateway Tax accounting

Passwords

The Ranch Weymouth takes the security of its passwords seriously and expects all employees to do the same.

Access to Office365 applications, including email and Sharepoint is via a complex password created and imputed by the in built security system of Microsoft and restricted. Any request from staff for a new password being actioned only by The Operational System Admin and Director and lead facilitator Toni Matthews. toni@theranchweymouth.com.

Office365 passwords are automatically reset when a user leaves the organisation, changes roles within the organisation, or will be absent from the organisation for an extended period of time, for example, on Maternity or Paternity Leave. Authorisation for a password to be reset by the Operational Systems Administrator will be given by Director Toni Matthews - Lead Facilitor. Email diverts or forwards also require the same authorisation.

Users are automatically prompted to change their lock screen password (desktop/laptop) at regular intervals.

The Ranch Weymouth follows guidance on Using Passwords from the National Cyber Security Centre, and also requires its employees to adhere to this guidance and the following requirements when using and setting passwords which are not controlled centrally by The Ranch Weymouth.

Passwords must:

- Use 2 Factor Authentication (where applicable/available)
- Avoid the most common passwords that criminals can easily guess, for example

‘passw0rd’.

- Must be longer than 8 digits long.
- Be made of up of 3 random words – these must not be words which are easily guessed (like a pet’s name or anything which is linked to The Ranch Weymouth, your hobbies, or your children). Numbers and symbols can be included if you need to, for example, ‘OrangeToasterExtension5!’.
- Not be duplicated/used for multiple accounts
- Not be written down and kept near to your computer. If passwords are written down, they must be kept securely, out of sight.

Passwords can be stored in your browser when prompted as this is more convenient and safer than re-using the same password.

If more than one person is accessing your computer, you should ideally have different accounts, and different passwords, for each person. Where this isn’t possible, make sure you know who has access to your devices, who knows the password, and that you have agreed to this.

Never write the password on a Post-it that’s stuck to the computer, where anyone could access your details. For the same reasons, use a **lock screen** when you’re not at your desk, and make sure you change your passwords when a member of staff with access to your devices leaves.

Employee Responsibilities

All employees of The Ranch Weymouth are responsible for ensuring they:

- Undertake all relevant training on Cyber Security issued to them by The Ranch Weymouth, including via links sent by The Ranch to the NSPCC online training.
- Use Sharepoint (and **not** email) to share any information of a sensitive information
- Include password protection on all documentation coming via emails i.e. safeguarding notifications, contracts of employment, parents refunds and a host of other email traffic attachments that contain personal data.
- Password protect any document which cannot be shared via Sharepoint before sending via email. Passwords must never be shared via email and must be given verbally only. The person supplying the password must telephone the recipient, and not provide the password on an incoming call.
- Adhere to the password requirements detailed in this policy.
- Validate any unusual or suspicious request for information made via email or SMS with a trusted contact, and report the suspicious activity as per the reporting process detailed in this policy.
- Do not provide information about any member of staff, child, or parent of the school on an incoming call to the school (even to confirm they are at your school or work for the Company). You should never assume a phone call is authentic just because someone knows your basic details such as name and address and you should never confirm a child/learner’s attendance at your school as you cannot be sure who you are talking to. Advise you will look into the request, and then you should return the call on a known contact number.

  The telephone contact numbers are held in the Unit 21 Office. The direct contact to the on role school for each of The Ranch Weymouth’s pupils will be displayed.

  Each young person also has the on role school contact number and named contact held on the secure register/database.
- Always save documents on OneDrive or to Sharepoint. Documents should never be saved on your desktop as these are not recoverable.
- Read and are familiar with the NCSC’s Staying Safe Online ‘Top Tips for Staff’.
- Read and are familiar with the NCSC’s ‘Business Email Compromise’ Fact Sheet.
- Implement safe storage of confidential paperwork in a locked cabinet.

- Never take confidential or sensitive information home.
- Never leave hardware open to sensitive content in a car or otherwise non-secure location.
- Have face-recognition access enabled on the mobile phone that you access the secure session notes and Sharepoint365, with a PIN code which is not easily guessed, for example birthdays or other memorable dates/number combinations must not be used.
- Will not delay applying updates to apps and your device's software. These updates include protection from viruses and other kinds of malware, and will often include improvements and new features. Applying software updates is one of the most important things you can do to protect your devices.
- Update all apps and your device's operating system when you're prompted. You can also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.
- If you think your device contains a virus (or any other type of malware), please read the NCSC's guidance on how to recover an infected device which is detailed below.

Cyber-attack incident management plan

The ICO (Information Commissioner's Office) has guidance on personal data breaches which sets out clearly how to respond to a suspected breach. The ICO is clear that you must report a notifiable breach to them 'without undue delay' and not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

The board of Directors, led by the Designated Safeguarding Lead Iain Woodbridge, must ensure that The Ranch Weymouth has an incident management plan that encompasses the stages below, and that the plan is implemented in the event of cyber attack or suspected cyber attack occurring:
Stage 1 - Containment and recovery – Immediately a cyber attack is discovered or suspected it must be reported to LADO for advice and follow the Working Together Framework - including the flowchart of reporting included later in this document.. The incident must be investigated utilising appropriate staff to mitigate damage and recover any data lost where possible.
Stage 2 -Assessment of the ongoing risk to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach / attack.
Stage 3 - Follow guidance from LADO to make the decision if this is reported to the ICO to consider if the cyberattack needs to be reported to regulators (for example the ICO / DfE) and/or colleagues/parents as appropriate.
Stage 4 - Evaluation and response to consider any improvements to data security and evaluate future threats to security reporting.
Where a cyber security incident may involve a personal data breach, the DSL will ensure the Data Breach Procedure is also followed including without limitation notifying immediately LADO and following the below guidance.

Consider team resilience and welfare
During a crisis, staff at all levels of your organisation will probably experience stress and uncertainty, which can be extremely detrimental. You should put their welfare and morale at the top of your response plan. The NCSC has guidance on staff welfare during an incident.
Incidents often start with an intense period of activity, but many also have a 'long tail' with the impact lasting for months. The team will need to make important decisions throughout, but particularly when you are working out how to rebuild and prevent future incidents. It's important to make sure that staff aren't exhausted.

Report it

And finally, you should report significant incidents to the NCSC and UK law enforcement who can provide support. This also enhances understanding of the threat landscape, helping to prevent further incidents and improve security for everyone.
Report your cyber incident using the UK government signposting tool which lets you know which organisations to notify, based on the circumstances of the incident.

Cyber Crime as an internal threat from young people

This section offers guidance which has a focus on offences committed by young people rather than external cybercrime and cyber security
Further guidance can be found at www.ncsc.gov.uk
Such as but not limited to:

Breaking IT rules

- **Unauthorised access to computers**
- **Denial of Service or other computer interference and impairment**
- **Acts causing serious damage to or loss of data**
- **'Hacking'**

The Ranch Weymouth should first establish:

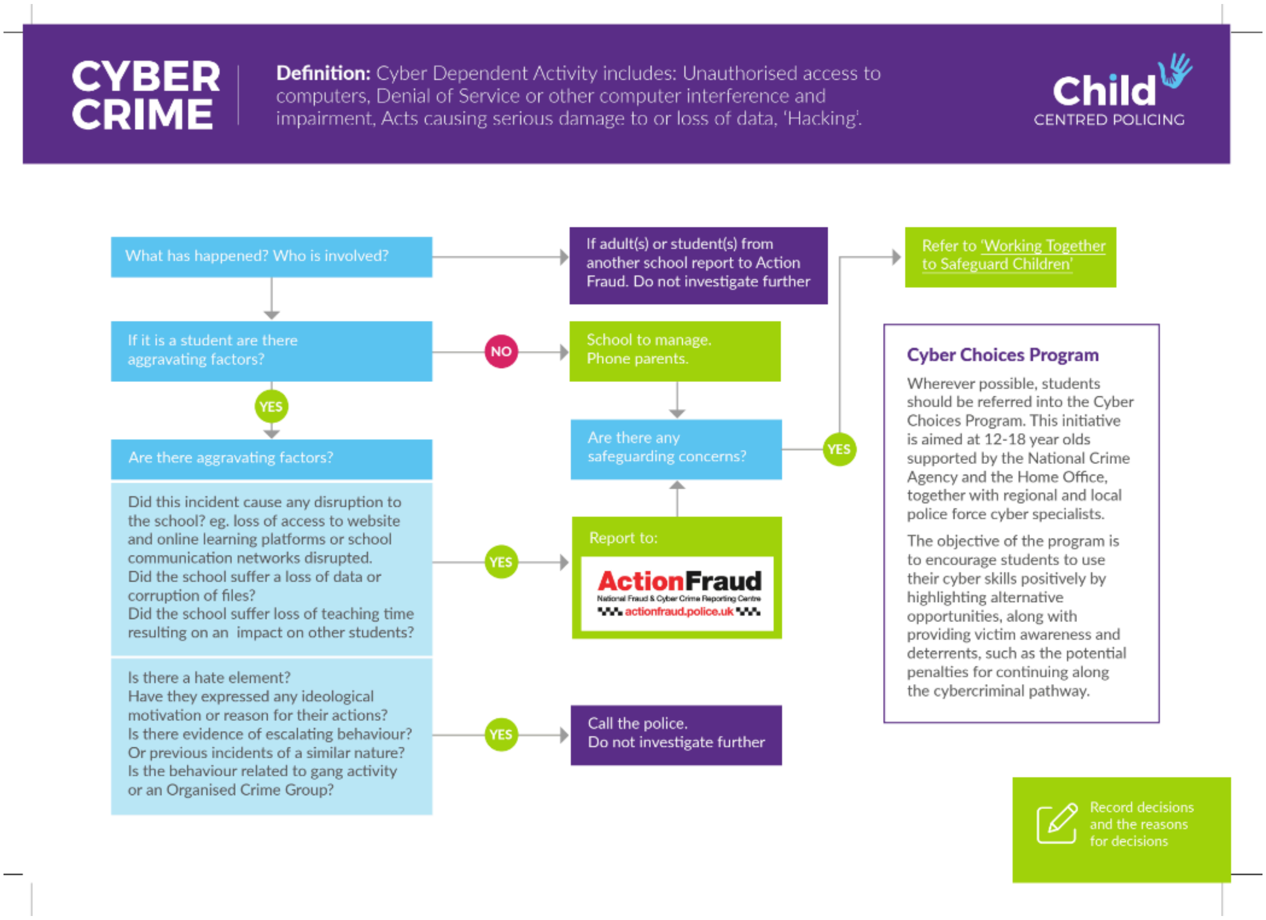
- What has happened?
- Who is involved?
- Is this part of a pattern of behaviour?
- Are there any safeguarding concerns? If YES — follow local safeguarding protocols

Are there any aggravating factors?

- Did this incident cause any disruption to The Ranch Alternative Provision? eg. loss of access to website and online learning platforms or communication networks disrupted.
- Did The Ranch suffer a loss of data or corruption of files?
- Did The Ranch suffer loss of teaching time resulting on an impact on other students?
- Is there a hate element?
- Have they expressed any ideological motivation or reason for their actions?
- Is there evidence of escalating behaviour? Or previous incidents of a similar nature?
- Is the behaviour related to gang activity or an Organised Crime Group?
- Do the young people involved have any additional relevant vulnerabilities?

Cyber Choices Program

Wherever possible, students should be referred into the Cyber Choices Program. This initiative is aimed at 12-18 year olds supported by the National Crime Agency and the Home Office, together with regional and local police force cyber specialists. The objective of the program is to encourage students to use their cyber skills positively by highlighting alternative opportunities, along with providing victim awareness and deterrents, such as the potential penalties for continuing along the cybercriminal pathway



CYBER CRIME

Definition: Cyber Dependent Activity includes: Unauthorised access to computers, Denial of Service or other computer interference and impairment, Acts causing serious damage to or loss of data, 'Hacking'.

Child CENTRED POLICING

What has happened? Who is involved?

If adult(s) or student(s) from another school report to Action Fraud. Do not investigate further

Refer to 'Working Together to Safeguard Children'

If it is a student are there aggravating factors?

NO

School to manage. Phone parents.

YES

Are there aggravating factors?

Are there any safeguarding concerns?

YES

Did this incident cause any disruption to the school? eg. loss of access to website and online learning platforms or school communication networks disrupted.
Did the school suffer a loss of data or corruption of files?
Did the school suffer loss of teaching time resulting on an impact on other students?

YES

Report to:

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Is there a hate element?
Have they expressed any ideological motivation or reason for their actions?
Is there evidence of escalating behaviour?
Or previous incidents of a similar nature?
Is the behaviour related to gang activity or an Organised Crime Group?

YES

Call the police.
Do not investigate further

Cyber Choices Program

Wherever possible, students should be referred into the Cyber Choices Program. This initiative is aimed at 12-18 year olds supported by the National Crime Agency and the Home Office, together with regional and local police force cyber specialists.

The objective of the program is to encourage students to use their cyber skills positively by highlighting alternative opportunities, along with providing victim awareness and deterrents, such as the potential penalties for continuing along the cybercriminal pathway.

Record decisions and the reasons for decisions

Lessons and Recommendations after local attacks on schools within Dorset

Strengthening Cybersecurity Infrastructure: Educational institutions must recognise the importance of investing in robust cybersecurity infrastructure. Regular audits, vulnerability assessments, and updates to security systems can help identify and mitigate potential weaknesses, reducing the risk of successful cyber attacks. Implementing multi-factor authentication, strong password policies, and encryption techniques can add additional layers of protection.

Cybersecurity Awareness and Training: Education on cybersecurity best practices should be integrated into the curriculum and provided to students, teachers, and administrative staff. Creating a culture of cybersecurity awareness can help prevent social engineering attacks, phishing attempts, and other common cyber threats. Regular training sessions and awareness campaigns can empower individuals to identify and respond effectively to potential risks.

Incident Response and Business Continuity Plans: Establishing comprehensive incident response plans is vital for educational institutions to minimise the impact of cyber attacks. These plans should outline the steps to be taken in the event of an attack, including communication protocols, data backup procedures, and strategies for maintaining essential operations. Regular drills and simulations can help test the effectiveness of these plans and ensure a swift response during real-world incidents.

Collaborative Efforts and Information Sharing: Schools should foster collaboration with cybersecurity experts, local authorities, and other educational institutions to exchange information, share best practices, and stay updated on emerging threats. Collaborative efforts can strengthen the collective resilience against cyber attacks and enable educational institutions to respond more effectively to evolving challenges.

Further Information and Reading

https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

https://www.ncsc.gov.uk/files/Recovering-hacked-online-accounts-infographic.pdf

Online Safety Advice:

- https://www.getsafeonline.org/
  UK's leading awareness resource helping to protect people from online fraud and other issues.

- https://www.cyberaware.gov.uk/
  Government advice about cyber security

- https://www.cyberessentials.ncsc.gov.uk/advice/
  Government advice for Businesses
- https://takefive-stopfraud.org.uk/
  Advice regarding online fraud (**Take Five campaign toolkit**)
- https://www.saferinternet.org.uk/
  Online safety tips, advice and resources

- https://www.ageuk.org.uk/information-advice/work-learning/technology internet/internet-security/
  Age UK advice and tips to stay safe online

- https://www.ncsc.gov.uk/information/report-suspicious-emails If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS).
- https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them securely
  Video conferencing guidance from the NCSC (**Individuals**)
- https://www.ncsc.gov.uk/guidance/video-conferencing-services-security guidance-organisations
  Video conferencing guidance from the NCSC (**Organisations**)
- https://www.actionfraud.police.uk/
  Action Fraud is the UK's national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland.
- https://www.ncsc.gov.uk/information/mailcheck
  NCSCs mail check assists with email reporting and configuration (DMARC). •
  Cyber Aware - NCSC.GOV.UK
  Step-by-step instructions on enabling the free security feature that prevents hackers from accessing your accounts, even if they know your password. •
  https://haveibeenpwned.com/
  Check if your accounts have been compromised.
- Social Media: how to use it safely - NCSC.GOV.UK
  Social Media Privacy Settings.

- Police CyberAlarm

Helping organisations monitor and report the malicious activity they face from the Internet

Useful Videos:

https://www.youtube.com/watch?v=sgs3lnemp3g&feature=youtu.be- Threat Actors

https://youtu.be/ZPori-GTI-4 - Ransomware

https://www.getsafeonline.org/fraudstars/ - Impersonation Fraud

https://www.youtube.com/watch?v=yrjT8m0hcKU – Action Fraud (Social Media Settings)

https://www.youtube.com/watch?v=aujUI3yt6nM – Quad9

Cyber Prevent Links:

https://www.youtube.com/watch?v=DjYrxzSe3DU- NCA Video.

Learn how to protect yourself online with the Cyber Aware Action Plan:- Individuals and families Action Plan - NCSC.GOV.UK