ICT Acceptable Use Policy

MINERVA'S
virtual academy

MINERVA'S
virtual academy

DEFINITIONS

In this Policy:

- **Staff** means all those working permanently or temporarily for or on behalf of the School (including those undertaking work experience, Board members and other volunteers) and may also include parents of students currently registered at the School.
- **School** means Minerva's Virtual Academy.
- **Student** means a student currently enrolled at Minerva's Virtual Academy.

This policy should be read in conjunction with other School policies, in particular the Safeguarding, Online Safety and Behaviour. Links can be found at the bottom of this policy

MINERVA'S
virtual academy

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works and is a critical resource for all members of the MVA community. As an online school, it is fundamental to our teaching and learning, safeguarding, pastoral and administrative functions of the school.

Maintaining system and device security is the responsibility of Head of Operations. Any concerns should be reported to the Head of Operations who will liaise with the Senior Leadership Team and DSL to ensure online safety and security measures are met.

However, the ICT resources and platforms our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct/etc.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000

- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- ICT facilities: all facilities, systems and services including, but not limited to, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service and platforms
- Users: anyone authorised by the school to use the school's ICT facilities, including, staff, pupils, volunteers, and visitors
- Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- Authorised personnel: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- Materials: files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities/platforms. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on the school's platforms without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the platforms, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities/platforms
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities/platforms is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

MVA's approach to the acceptable use of artificial intelligence (AI) tools:

- Pupils may use AI tools and generative chatbots:
- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour/discipline/staff discipline/staff code of conduct.

Sanctions in place for unacceptable ICT use include revoking permission to use the school's systems and suspensions of access to Canvas, school gmail account, Big Blue Button.

5. Staff

5.1 Access to school ICT facilities/platforms and materials

The school's Operations Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, mobile phones and other devices
- Access permissions for certain platforms, programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT systems and platforms.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Operations Manager.

Staff who are provided with MVA equipment must adhere to SonarIT Cyber Security protocols along with all other protocols referenced in this policy.

Staff must use 2FA to access iSAMs and CPOMs.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must use a separate user account for access to MVA platforms and systems.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Operations Manager mmediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones (including the Voiphone app) provided by the school to conduct all work-related business.

School phones/voiphone app must not be used for personal matters.

Staff who are provided with mobile phones/voiphone as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The school can record incoming and outgoing phone conversations.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so. Your school's phone system probably has an automated option you can use/adapt.

Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to Operations Manager or Headteacher.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

The Headteacher or Head of Operations may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEND) assessments, etc.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher] may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the rules layed out in this policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 School social media accounts

The school has an official Facebook/Instagram/LinkedIn] account, managed by the Social & Community Manager and Head of Growth. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.4 Monitoring and filtering of the use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities/platforms. This includes, but is not limited to, the filtering and monitoring of:

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

MINERVA'S
virtual academy

At Minerva Virtual Academy (MVA), we understand the importance of maintaining a safe online environment for our students. Given that our students access lessons from home, we acknowledge the limitations faced by our staff in preventing access to inappropriate websites. Therefore, we rely heavily on the cooperation of parents, carers, and mentors to monitor the online activity of their children or young people.

We strongly recommend to all families that a practice of filtering and monitoring take place at home ensuring that the websites, applications, and programmes used are suitable for the students' age and experience.

Parents, carers, and families must be vigilant in monitoring online activities to safeguard children and young people. Alongside online safety workshops, hosted by the NSPCC, parents are encouraged to familiarise themselves with:

https://www.iwf.org.uk/

https://www.ceop.police.uk/safety-centre/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

In the event that any staff or students discover an unsuitable site shared or posted on MVA platforms, it must be reported to a member of the senior leadership team immediately. We will report any online material believed to be illegal to the relevant authorities.

MVA recognises the role of the Internet Watch Foundation and encourages parents and carers to prevent access to sites listed by the IWF. Parents, carers, and mentors will be informed of any breaches in behaviour, safeguarding, anti-bullying, and e-safety policies involving their children or young people.

MVA will review these standards regularly and work with IT staff and service providers to enhance support for schools and colleges in meeting these essential requirements.

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Head of Operations, as appropriate.

5.5 Bring Your Own Device

The primary use of personal devices at Minerva Virtual Academy (MVA) is strictly for educational or business purposes. Users must have a comprehensive understanding of how to operate their devices and are responsible for their upkeep.

Personal devices must adhere to MVA's Acceptable Use Policy. Additionally, photographing or video recording without permission is strictly prohibited to maintain privacy and security.

Regarding liability, users bring personal devices to MVA at their own risk. The academy is not responsible for the upkeep, security, damage, loss, or malfunction of any personal devices. Furthermore, MVA does not provide technical support for personal devices, so users must be prepared to manage their devices independently.

Personal devices should not contain inappropriate software or display offensive content, ensuring a safe and respectful environment for all members of the academy.

6. Pupils

6.1 Access to ICT facilities

Primarily students accessing MVA platforms use personal devices. On the rare occasion students are provided with an MVA device they are not permitted to use the device for personal use.

6.2 Search and deletion

Under the Education Act 2011, the Headteacher, DSL and any member of staff authorised to do so by the Headteacher, can request parents/carers to search students' devices and remove access to all MVA platforms if they or and other member of staff has reasonable grounds for suspecting students are accessing or sharing content and/or information which:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out as listed in our behaviour policy, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher and or DSL
- Explain to the pupil why their access to MVA platforms is being removed and parents/carers are being asked to search their devices, and give them the opportunity to ask questions about it
- Seek the parents or carers cooperation in providing the student's necessary login information,

The authorised staff member should:

- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files within the MVA platforms where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found, it is up to the DSL and Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the material will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Remove user access from all MVA platforms and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT

The school will sanction pupils, in line with the Behaviour Policy if a pupil engages in any of the following **at any time**):

- Using ICT/school's platforms to breach intellectual property rights or copyright
- Using ICT /school's platforms to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the school's systems, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities/live lessons

- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Causing significant disruption to live lessons by inappropriate use of technology
- Any other breach of the Behaviour Policy or Online Safety Policy

6.4 Bring Your Own Device (as referenced in 5.5 above)

- The primary use of personal devices at Minerva Virtual Academy (MVA) is strictly for educational or business purposes. Users must have a comprehensive understanding of how to operate their devices and are responsible for their upkeep.
- Personal devices must adhere to MVA's Acceptable Use Policy. Additionally, photographing or video recording without permission is strictly prohibited to maintain privacy and security.
- Regarding liability, users bring personal devices to MVA at their own risk. The academy is not responsible for the upkeep, security, damage, loss, or malfunction of any personal devices. Furthermore, MVA does not provide technical support for personal devices, so users must be prepared to manage their devices independently.
- Personal devices should not contain inappropriate software or display offensive content, ensuring a safe and respectful environment for all members of the academy.

7. Parents / Carers

7.1 Access to ICT Systems & Platforms

Parents/carers have access to Canvas and the parent portal hosted by iSAMS. Although this access is limited parents are expected to follow all the same protocols laid out in this policy.

As students study at home parents/carers may have access to student login information. In this case they must abide by all rules laid out in this policy.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school or other parents through our website, social media channels and the Classlist parent app.

We ask parents/carers to review the agreement in appendix 2. By enrolling their child at MVA parents/carers are confirming that they agree to this acceptable use policy. Any parent/carer suspected of breaking this agreement risk their child being removed from the school.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of how students are expected to engage in Canvas and use of the school gmail.

Parents/carers will know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

We encourage all parents and carers to familiarise themselves with the MVA Online Safety Policy. For questions, concerns or advice, they should contact the Head of Operations who will consult with the senior leadership team where necessary.

8. Guests, Visitors and Volunteers

Any guests, visitors or volunteers will not be granted access to any MVA platforms apart from the live link needed to attend the meeting / workshop / lesson agreed.

Once their meeting has taken place this link will be closed down and access denied.

9. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

MVA has taken steps to ensure the safety and security of their systems by contracting SonarIT Services to manage Cyber Security measures. Any student, parent/ guardian or member of staff who wish to speak directly with SonarIT can do so by contacting the Head of Operations.

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Students and staff have individual school logins. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:
• use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every three months;
• not write passwords down;
• not share passwords with other students or staff; and
• use of two-factor authentication (code via App/SMS) for CPOMs and iSAMs

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

9.2 Software updates, firewalls and anti-virus software

Where personal devices are in use students and parents/guardians are responsible for for ensuring their devices are up to date and they have anti-virus software in plac.

All staff using either MVA provided equipment or personal devices must liaise with SonarIT Services to enstall the following software provided:

- Patch Management: This is the controlled updates of devices and applications. This prevents cyber criminals from being able to exploit MVA through outdated systems such as Web browsers, operating systems and other applications.
- Centrally Managed Anti-Virus: Centrally managed anti-virus ensures the devices are running quickly and deep scans, actively updating definitions to ensure devices are protected. The Anit-Virusis compatible with Chromebook's, Mac, and Windows
- Cloud Backup: For anything which sits within Google Education Suite to ensure data is backed up

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

9.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by Head of Operations.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert Head of Operations immediately.

Users should always log out of systems when they are not in use to avoid any unauthorised access. Systems should always be logged out of completely at the end of each working day.

10. Protection from Cyber Attacks

The school will:

- Work with the operations department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Back up critical data regularly and store these backups on cloud-based backup system as provided by SonarIT
- Delegate specific responsibility for maintaining the security of all our systems and school devices including management information system (MIS) to Head of Operations
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like our MIS
    - Store passwords securely and change them regularly
- Make sure the operations team conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

11. Internet Access

As an online, remote school, it is the responsibility of MVA staff and parents/carers to ensure that all staff and students have access to fast / reliable wi-fi connectivity.

12. Monitoring and Review

The Headteacher and Head of Operations monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This procedure is designed to set good practice standards. However, the School recognises that best practice develops over time and, as such, will update it regularly in the light of experience and as a result

of changes in legislation or its own internal organisation and policies. The procedure will be subject to a comprehensive review on an annual basis.

Date Policy created:	February 2022
Last Review Date: Reviewed by:	February 2024 Chloe Wiliams, Head of Operations Suzanne Lindley, Headteacher
Next Review Date:	February 2025

Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Data protection

MINERVA'S
virtual academy

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

MINERVA'S
virtual academy

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so
- Contact a member of senior leadership or the headteacher if you are unsure about whether you would like to respond

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

MINERVA'S
virtual academy

Appendix 2: Acceptable use of MVA Systems & Platforms: agreement for parents and carers

Acceptable use of MVA Systems & Platforms: agreement for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform
- Classlist

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. This primarily takes place on Classlist so that private contact details do not need to be shared.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

By enrolling your child at MVA you agree to these terms

MINERVA'S
virtual academy

Appendix 3: Acceptable use agreement for students

Acceptable use of the school's ICT facilities, systems & platforms: agreement for students

When using the school's ICT systems and platforms, I will not:

- Use them for a non-educational purpose
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails which have been sent by an external source, unless advised by my teacher
- Use any inappropriate language when communicating online, including in emails, live lesson chat and canvas messager
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

I understand that the school can monitor my access to MVA platforms and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and platforms responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

By being enrolled at MVA you agree to follow the rules above

MINERVA'S
virtual academy

Appendix 4: Acceptable use agreement for staff

Acceptable use of the school's ICT facilities, systems & platforms: agreement for staff, volunteers and visitors
When using the school's ICT systems and platforms I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Use any improper language when communicating online, including in emails or other messaging services • Install any software, or connect hardware or devices to my device which may impact the systems and platforms used by MVA • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school
I understand that the school can monitor my access to MVA platforms and systems. I will take all reasonable steps to ensure that my devices are secure and password-protected and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and headteacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's systems and platforms responsibly, and ensure that pupils in my care do so too.
By working for or with MVA all staff, volunteers and visitors agree to these terms

MINERVA'S
virtual academy

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

MINERVA'S
virtual academy

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.