ICT, Internet Acceptable Use and Social Media Policy

Strive for Education

Approved by:	**S Brown**	**Creation Date:**	**August 2021**
Last reviewed on:	**February 2024**	**Next review date:**	**February 2025**

Contents

1. Introduction and aims

Our Information and Communication Technology (ICT) systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

Sonja Brown, Operations Director, has overall responsibility for this policy, including keeping it under review.

Breaches of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

ICT is an integral part of the way Strive works, and is a critical resource for students, staff, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions. However, the ICT resources and facilities Strive uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Strive ICT resources for staff, students and parents
- Establish clear expectations for the way all members of the Strive community engage with each other online
- Support Strives policy on data protection, online safety and safeguarding
- Prevent disruption to Strive through the misuse, or attempted misuse, of ICT systems
- Support Strive in teaching students safe and effective internet and ICT use

This policy covers all users of Strive's ICT facilities, including staff, students, volunteers, contractors and visitors.

2. Relevant legislation and guidance

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

- Data Protection Act 2018 and UK GDPR
- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools

3. Definitions

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

4. Unacceptable use

The following is considered unacceptable use of Strive's ICT facilities by any member of the Strive community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of Strive's ICT facilities includes:

- Using Strive's ICT facilities to breach intellectual property rights or copyright
- Using Strive's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching Strive's policies or procedures
- Any illegal conduct, or 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

Activity which defames or disparages Strive, or risks bringing Strive into disrepute:

- Sharing confidential information about Strive, its students, or other members of Strive's community
- Connecting any device to Strive's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Strive's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, 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 Strive's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to Strive
- Using websites or mechanisms to bypass the Strive's filtering mechanisms

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

Exceptions from unacceptable use

Where the use of Strive ICT facilities 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.

Any individual who requires to use the ICT facilities in a way which may be considered unacceptable will be required to gain written approval from the Headteacher.

Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with Strive's policies on staff code of conduct.

Our Staff Code of Conduct policy will have been supplied to you during your induction, this is a link to the Staff Information area on SharePoint where you can access it. LINK HERE

5. Staff (including advisers, volunteers, and contractors)

Access to Strive's ICT facilities and materials

Strive's Operation Director Sonja Brown, alongside an external IT Contractor manages access to Strive's ICT facilities and materials for Strive staff. That includes, but is not limited to:

- Computers, tablets, iPads and other devices
- Access permissions for certain programmes or files
- Staff will be provided with log-in/account information and passwords that they must use when accessing the Strive's ICT facilities.
- Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Operations Director or Headteacher, Andy Brown.

Use of phones and email

Strive provides each permanent 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 Strive has provided.

Staff must not share their personal email addresses with parents and students 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 and UK GDPR 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 you are unsure whether the information you are sending is going to be protected in transit always check before sending.

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 which contains the personal information of another person, they must inform the Operations Director immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by Strive to conduct all work-related business.

Strive phones must not be used for personal matters, unless prior authorisation is received from the Headteacher or suitably senior colleague.

Strive can record in-coming and out-going phone conversations, however this is not done as standard.

Staff who would like to record a phone conversation should speak to the Andy Brown, the Headteacher.

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

Our protocol for approving requests is listed here. We may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.
- Discussing requests for term-time holidays

6. Staff use

Staff are permitted to occasionally use Strive's ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Operations Director may withdraw permission for it at any time or restrict access 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 students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use the Strive'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 Strive's ICT facilities for personal use may put personal communications within the scope of Strive's ICT monitoring activities. 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 Strive's Mobile Phone policy.

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

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

Personal social media accounts

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

Remote access

We may allow staff to access Strive's ICT facilities and materials remotely. This is subject to requirements and roles. Anybody requiring remote access to the Strive's ICT facilities should contact the Operations Director or Headteacher.

Staff accessing Strive's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use Strive's ICT facilities outside of the Strive building and take such precautions as the Operations Director / Headteacher may require from time to time against importing viruses or compromising system security. Staff are supplied with a Strive owned computer, staff are not permitted to use their own computer or device such as iPads.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Additional 'multi-factor' authentication must be set up to access all Strive systems and documents. This will be set as standard by the IT contractor, however if there is an issue with this or staff notice that they are able to log-in to a system without entering additional multi-factor authentication information – the staff member must report this to Sonja Brown.

Strive's social media accounts

Strive has official Twitter and Facebook accounts, these are managed by the Operations Director, Headteacher and other can be approved. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Strive has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of Strive's network and use of ICT facilities

Strive reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- Only authorised personnel may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

Strive monitors ICT use in order to:

- Obtain information related to Strive business
- Investigate compliance with Strive policies, procedures and standards
- Ensure effective business 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

7. Student use

Access to ICT facilities

Computers and equipment at Strive are available to students only under the supervision of staff. Students must log-in to laptops with their own log-in details, this is extremely important in order to keep our students safe. Chromebooks should be 'booked out' at the beginning of lessons and signed back in at the end of lessons, this is because a generic log-in is currently used so we must be able to identify which student had which Chromebook when. Staff will note the number of the device and which student is using it. Logging this enables Strive to monitor activity on the devices such as internet searches, this is important for us to be able to keep our students safe and to identify any areas of concern.

Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

Students cannot access the Strive's Wifi on their personal devices such as phones / iPads etc.

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, Strive has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under Strive rules or legislation.

Strive can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break Strive's rules. See Strive's Searching and Screening Policy.

Unacceptable use of ICT and the internet outside of Strive

Strive will sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on Strive's premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching Strive's policies or procedures
- Any illegal conduct, or 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

Activity which defames or disparages Strive, or risks bringing Strive into disrepute.

Sharing confidential information about Strive, other students, or other members of the Strive community

Gaining or attempting to gain access to restricted areas of the network, 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 Strive's ICT facilities

Causing intentional damage to ICT facilities or materials

Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

Using inappropriate or offensive language

We ask students to sign the agreement within the Google Enrolment Form.

8. Parent use

Access to ICT facilities and materials

Parents do not have access to Strive's ICT facilities as a matter of course.

However, parents working for, or with, Strive in an official capacity (for instance, as a volunteer or as a member of the PTA (when one is established)) may be granted an appropriate level of access, or be permitted to use Strive's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about Strive online

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

Parents play a vital role in helping model this behaviour for their children, especially when communicating with Strive through our website and social media channels.

We ask parents to sign an agreement within the Enrolment Form.

9. Data security

Strive takes steps to protect the security of its computing resources, data and user accounts. However, Strive cannot guarantee security. Staff, students, parents and others who use Strive's ICT facilities should use safe computing practices at all times.

Equipment security and passwords
You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office, do not save those passwords. You should keep your passwords confidential and change them regularly.

You must only log on to our systems using the login credentials assigned to you. You must not use another person's username and password or allow anyone else to log on using your username and password.

If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

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

Passwords should be updated regularly and multi-factor authentication should be used.

Software updates, firewalls, and anti-virus software

All of Strive's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly and where possible automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and Strive's ICT facilities.

Personal computer devices are not to be used to access the Strive network.

10. Data protection

All personal data must be processed and stored in line with data protection regulations and Strive's Data Protection Policy.

Access to facilities and materials

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

These access rights are managed by the Operations Director.

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 the Operations Director or Headteacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day or when finished with.

When using a Strive computer staff should log in to the Staff laptop profile and not as a student.

Encryption

Strive ensures that its devices and systems have an appropriate level of encryption.

It should not be necessary for staff to use their personal devices (computers) to access the Strive data, when working remotely staff should use their Strive owned and issued laptop.

USB memory drives are not permitted to be used, should a staff member require to use one they should seek permission from Andy or Sonja Brown.

11. Internet access

Strive's wireless internet connection is secured.

Our Wifi uses filtering, this is for the safety of our students.

As we use filtering, please be aware that filters aren't fool-proof. If you are made aware of access to inappropriate sites that the filter hasn't identified or equally appropriate sites that have been filtered in error please report this to the Headteacher or the Operations Director.

Further information is within the Acceptable use of the internet policy in Appendix 2, 3 and 4.

Students

Students cannot gain access to Strive's Wifi on their personal devices.

Parents and visitors

Parents and visitors to Strive will not be permitted to use the Wifi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with Strive in an official capacity (e.g. as a volunteer or as a member of the PTA (when one is established))
- Visitors need to access Strive Wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

12. Social media policy - Staff

About this policy
This policy is in place to minimise the risks to our business through use of social media.

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram, Snapchat and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Personal use of social media
Personal use of social media on any device is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

Prohibited use
You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.

You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

Any misuse of social media should be reported to Andy Brown, Headteacher.

Guidelines for responsible use of social media

You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

If you see social media content that disparages or reflects poorly on us, you should contact Andy Brown or Sonja Brown.

Breaches of this policy

Breaches of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

13. Monitoring and review

The Headteacher and Operations Director monitor the implementation of these policies, including ensuring that it is updated to reflect the needs and circumstances of Strive.

The ICT, Internet Acceptable use and Social Media policies will be reviewed every year.

Related policies

This policy should be read alongside Strive's policies on:

- Safeguarding and Child Protection
- Behaviour and Positive Relationships
- Staff Handbook
- Staff Code of Conduct
- Data Protection Policy
- Student Confidentiality Policy
- Privacy Notices
- Mobile Phone Policy

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from students on social media

10 rules for Strive staff on Facebook and other social media channels

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 not, ensure 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 just as happy showing your students
6. Don't use social media sites during your Strive working hours
7. Don't make comments about your job, your colleagues, Strive, or your students online – once it's out there, it's out there
8. Don't associate yourself with Strive on your profile (e.g. by setting it as your workplace, or by 'checking in' at a Strive 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 students)

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students 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

What do to if...

A student adds you on social media

In the first instance, ignore and delete the request. Block the student from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages

Notify the Headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at Strive

Students may then have indirect access through their parent'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 know that you're doing so

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 student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent 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

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

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

Strive uses the following channels:

- Our official Twitter account @EducationStrive
- Our official Facebook page www.facebook.com/EducationStrive
- Email/text groups for parents (for Strive announcements and information)
- Our website

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

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

I will not:

- Use private groups, Strive's Twitter account or personal social media to complain about or criticise members of staff. This is not constructive and Strive can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, Strive's Twitter account, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact Strive 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 other children's parents/carers

Appendix 3: Acceptable use agreement for older students

Acceptable use of Strive's ICT facilities and internet: agreement for students and parents/carers

When using the Strive's ICT facilities and accessing the internet at Strive, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break Strive 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, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to Strive's network using someone else's details
- Bully other people

I understand that Strive will monitor the websites I visit and my use of Strive's ICT facilities 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 Strive's ICT systems and internet responsibly.

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

Appendix 4: Acceptable use agreement for staff, advisers, volunteers and visitors

Acceptable use of Strive's ICT facilities and the internet: agreement for staff, advisers, volunteers and visitors

When using Strive's ICT facilities and accessing the internet at Strive, or outside Strive on a work device, 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 Strive's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to Strive's network
- Share my password with others or log in to Strive's network using someone else's details
- Share confidential information about Strive, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to Strive

I understand that Strive will monitor the websites I visit and my use of Strive's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside Strive, and keep all data securely stored in accordance with this policy and Strive's data protection policy.

I will let the designated safeguarding lead (DSL) and Headteacher know if a student 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 Strive's ICT systems and internet responsibly and ensure that students in my care do so too.