ICT and Internet Acceptable use Policy

Approved by:	[Lindsay Nicoll]	**Date:** [08.01.25]
Last reviewed on:	[08.01.25]	
Next review due by:	[08.01.27]	

Contents

---

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our company works, and is a critical resource for pupils, staff (including the management team), volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the business.

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

This policy aims to:

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

Breaches of this policy may be dealt with under our Staff Code of Conduct policy.

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 businesss 2022
- National Cyber Security Centre (NCSC): Cyber Security for Businesss
- 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 businesss and colleges
-

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, 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 companies ICT service
- **Users:** anyone authorised by the company to use the companies ICT facilities, including staff, pupils, volunteers, contractors 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 business to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the companies 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 companies ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the companies ICT facilities includes:

- Using the companies ICT facilities to breach intellectual property rights or copyright
- Using the companies ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the companies 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 business, or risks bringing the business into disrepute
- Sharing confidential information about the business, its pupils, or other members of the business community
- Connecting any device to the companies ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the companies network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the companies 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 the companies ICT facilities
- Causing intentional damage to the companies ICT facilities
- Removing, deleting or disposing of the companies 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 business
- Using websites or mechanisms to bypass the companies filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

5. Staff (including volunteers, and visitors)

5.1 Access to business ICT facilities and materials

The management team manage access to the companies ICT facilities and materials for business staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices

- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the companies ICT facilities. Evolve Technologies support our ICT infrastructure and are available for support throughout the working day.

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 their Operations Manager to be provided with access.

5.2 Use of phones and email

The business provides each staff member with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

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

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 their AP Manager immediately and follow our data breach procedure.

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

Business phones must not be used for personal matters.

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

5.3 Personal use

Staff are permitted to occasionally use business ICT facilities for personal use in cases of an emergency. This permission must not be overused or abused. The management team may withdraw or restrict this permission at any time and at their discretion.

Staff may not use the companies 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 companies ICT facilities for personal use may put personal communications within the scope of the companies ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using business 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.

5.3.1 Personal social media accounts

Staff should take care to follow the companies procedures on use of social media (see appendix 1) to protect themselves online and avoid compromising their professional integrity.

5.4 Remote access

We allow staff to access the companies ICT facilities and materials remotely.

Staff accessing the companies 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 the companies ICT facilities outside the business and must take such precautions to protect against importing viruses or compromising system security.

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. This policy is accessible via our website - https://oakactivities.com/knowledge-hub/

5.5 Business social media accounts

The business has an official Facebook, Instagram and LinkedIn account, managed by Holly Piaggesi, Hayley Twyneham and Tom Milner. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The business 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.

5.6 Monitoring and filtering of the business network and use of ICT facilities

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

- Internet sites visited
- 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 business monitors ICT use in order to:

- Obtain information related to business
- Investigate compliance with business 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

The Business and Compliance Manager is responsible for making sure that:

- The business meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the management team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the companies monitoring and filtering systems

Where appropriate, staff may raise concerns about monitored activity with the companies DSL and Operations Managers, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment are available to pupils in some settings, only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or construction, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the companies ICT infrastructure to allow access to basic Microsoft platforms and the internet.
- Post 16 pupils can use the computers independently, for educational purposes only

6.2 Search and deletion

Under the Education Act 2011, the management team, and any member of staff authorised to do so by the management team, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the business rules as a banned item for which a search can be carried out **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 their AP Manager, or Operations Manager
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Inform parents of the need to conduct a search and seek co-operation
- Seek the pupil's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- 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 on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, 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 business or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL & management team 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 from a device, 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 device 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
- Confiscate the device 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

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

6.3 Unacceptable use of ICT and the internet outside of business

The business will place consequences in place for pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** while on business 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 the companies 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 business, or risks bringing the business into disrepute
- Sharing confidential information about the business, other pupils, or other members of the business 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 the companies ICT facilities
- Causing intentional damage to the companies 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
- Taking photographs or making video content of pupils, staff members of the setting without permission

7. Data security

The business 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 companies 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 businesss and colleges, including the use of:

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

8. Passwords

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

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.

8.2 Software updates, firewalls and anti-virus software

All of the companies ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or 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 the companies ICT facilities.

Any personal devices using the companies network must all be configured in this way.

8.3 Data protection

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

The data protection policy can be found here - https://oakactivities.com/knowledge-hub/

8.4 Access to facilities and materials

All users of the companies ICT facilities will have clearly defined access rights to business systems, files and devices.

These access rights are managed by the management team.

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 their line manager 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 shut down completely at the end of each working day.

8.5 Encryption

The business makes sure that its devices and systems have an appropriate level of encryption.

Staff may only use personal devices (including computers and USB drives) to access business data, work remotely, or take personal data (such as pupil information) out of business if they have been specifically authorised to do so by the management team.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The business will:

- Work with our IT department, Evolve Technologies, to make sure cyber security is given the time and resources it needs to make the business secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the companies annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for personal information or login details
- 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
- Put controls in place that are:
    - **Proportionate**: the business will verify this using a third-party audit to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the business needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like business email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the business has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- 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 business 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.

10. Internet access

Parents/carers and visitors

Parents/carers and visitors to the business will not be permitted to use the companies WiFi unless specific authorisation is granted by the management team.

The management team will only grant authorisation if:

- Parents/carers are working with the business in an official capacity (e.g. as a volunteer)

- Visitors need to access the companies WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation)

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

11. Monitoring and review

The management team monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the business.

This policy will be reviewed every 2 years and will be updated as and when necessary developments take place.

12. Related policies

This policy should be read alongside the companies policies on:

- Safeguarding and child protection
- Behaviour
- Staff Code of Coduct
- Data Protection

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for business 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 business hours
7. Don't make comments about your job, your colleagues, our business or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the business on your profile (e.g. by setting it as your workplace, or by 'checking in' at a business 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

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 management team and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the management team team or the management team 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 business
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- The request must be declined or you should ignore the message, consider drafting a stock response to let the parent/carer 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 pupil or staff member, report this to the management team for support.
- 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

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

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our business. The business uses the following channels: • Email to pupils key worker and AP Manager • AP Manager contact number • Our official Facebook page, Instagram page and LinkedIn page • Class Dojo for Primary pupils	
When communicating with the business via official communication channels, or using private/independent channels to talk about the business, I will: • Be respectful towards members of staff, and the business, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the companies official channels, so they can be dealt with in line with the companies complaints procedure I will not: • Use private groups, the companies Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the business can't improve or address issues unless they are raised in an appropriate way • Use private groups, the companies Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the business 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	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the companies ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the companies ICT facilities and accessing the internet in business, 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 business 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 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 companies network using someone else's details • Bully other people I understand that the business will monitor the websites I visit and my use of the companies 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 the companies ICT systems and internet responsibly. I understand that the business will put consequences in place if I do certain unacceptable things online, even if I'm not in business when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the companies ICT systems and internet when appropriately supervised by a member of business staff. I agree to the conditions set out above for pupils using the companies ICT systems and internet, and for using personal electronic devices in business, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, volunteers and visitors

Acceptable use of the companies ICT facilities and the internet: agreement for staff, volunteers and visitors	
Name of staff member/volunteer/visitor:	
When using the companies ICT facilities and accessing the internet in business, or outside business 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 the companies 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 the companies network • Share my password with others or log in to the companies network using someone else's details • Share confidential information about the business, 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 business	
I understand that the business will monitor the websites I visit and my use of the companies ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside business, and keep all data securely stored in accordance with this policy and the companies data protection policy. I will let the designated safeguarding lead (DSL) and my line manager 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 companies ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the business 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.

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.