

# ICT and internet acceptable use policy

All-Inspired Ltd



Approved by:	The relevant officer	Date: February 2024
Last reviewed on:	February 2024	
Next review due by:	February 2025	

# Contents

1. Introduction and aims	2
2. Relevant legislation and guidance	4
3. Definitions	3
4. Unacceptable use	3
5. Staff (including employers, volunteers and contractors)	4
6. Young people	7
7. Parents	8
8. Data security	8
9. Protection from cyber attacks	8
10. Internet access	10
11. Monitoring and review	11
12. Related policies	11
Appendix 1: Facebook cheat sheet for staff	12
Appendix 2: Acceptable use of the internet: agreement for parents and carers	14
Appendix 3: Acceptable use agreement for older young people	15
Appendix 4: Acceptable use agreement for younger young people	16
Appendix 5: Acceptable use agreement for staff, employers, volunteers and visitors	17
Appendix 6: Cyber security glossary.....	20

---

## 1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our business works, and is a critical resource for young people, and staff. It supports teaching and learning, pastoral and administrative functions of the business.

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

This policy aims to:

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

This policy covers all users of our business's ICT facilities, including employers, staff, young people, and school staff.

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 General Data Protection Regulation](#)
- › [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 2021](#)
- › [Searching, screening and confiscation: advice for businesses](#)
- › [National Cyber Security Business \(NCSC\)](#)
- › [Education and Training \(Welfare of Children Act\) 2021](#)

## 3. Definitions

- › **“ICT facilities”**: includes 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 which may become available in the future which is provided as part of the ICT service.
- › **“Users”**: anyone authorised by the business to use the ICT facilities, including employers, staff, young people and school staff.
- › **“Personal use”**: any use or activity not directly related to the users’ employment, study or purpose.
- › **“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 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 business’s ICT facilities by any member of the business community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the business’s ICT facilities includes:

- › Using the business’s ICT facilities to breach intellectual property rights or copyright.
- › Using the business’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- › Breaching the business’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 (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, its young people, or other members of the business community
- Connecting any device to the business's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the business'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 the business'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 has a legal contract or is directly related to the business.
- Using websites or mechanisms to bypass the business's filtering mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic 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 directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the business's ICT facilities.

#### **4.1 Exceptions from unacceptable use**

Where the use of business ICT facilities (on the business premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Directors' discretion.

Advice from the ICT manager would be taken in these circumstances.

#### **4.2 Sanctions**

Young people and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the business's policies on behaviour/discipline/staff discipline/staff code of conduct/etc.

Unacceptable ICT use may involve revoking permission to use the business's systems.

The business's behaviour policy, staff discipline policy, and staff code of conduct policies can be found on the SSF website.

## **5. Staff (including employers, and school staff.)**

### **5.1 Access to business ICT facilities and materials**

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

- › Computers, tablets, VR sets and mobile phones and other devices
- › Access permissions for certain programmes or files

Staff and students will be provided with unique log-in/account information and passwords that they must use when accessing the business'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 ICT manager via email or telephone.

#### 5.1.1 Use of phones and email

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

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

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 and young people 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 ICT manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or young people. 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.

The business can record in-coming and out-going phone conversations.

When we record calls, callers **ARE** made aware that the conversation is being recorded and the reasons for doing so. The business's phone system has an automated option we can use/adapt.

We will explain when you record phone conversations and why. For instance:

- › "All calls to the business 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 Directors.

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

We will 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 (SEN) assessments, etc.
- Discussing requests for term-time holidays

## 5.2 Personal use

Staff are permitted to occasionally use business ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The ICT manager 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 young people are present.
- Does not interfere with their jobs or prevent other staff or young people from using the facilities for work or educational purposes.

Staff may not use the business'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 business's ICT facilities for personal use may put personal communications within the scope of the business'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 business's mobile phone/personal device policy.

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 young people and parents could see them.

Staff should take care to follow the business's guidelines on 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 ensure their use of social media, either for work or personal purposes, is appropriate at all times.

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

## 5.3 Business social media accounts

The business has an official Facebook/Twitter/Linked in etc. page. 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 can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

## 5.4 Monitoring of business network and use of ICT facilities

The business 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 ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The business monitors ICT use 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.

## 6. Young people

### 6.1 Access to ICT facilities

- Computers, VR and equipment in the business's ICT suite are available to young people only under the supervision of staff.
- Young people will not be provided with an account – the staff will sign the computers on each session and supervise the young people.
- Young people can use the computers independently for educational purposes only

### 6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's [guidance on searching, screening and confiscation](#), the business has the right to search young people's phones, computers or other devices for pornographic images or any other data or items banned under business rules or legislation.

The business 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 the business's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

### 6.3 Unacceptable use of ICT and the internet outside of business

The business will sanction young people, in line with the behaviour/discipline policy, if a pupil engages in any of the following **at any time** (even if they are not 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 business'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.
- Consensual and 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 young people, 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 business'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

If the young people do any of the above, please see section 4.2 and our business's behaviour/discipline policy on the website.

## 7. Parents

### 7.1 Access to ICT facilities and materials

Parents do not have access to the business's ICT facilities as a matter of course. Unless the school has subscribed to the workplace visit website.

### 7.2 Communicating with or about the business online

We believe it is important to model for young people, 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 the business through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

## 8. Data security

The business is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the business cannot guarantee security. Staff, young people, parents and others who use the business's ICT facilities should use safe computing practices at all times.

### 8.1 Passwords

All users of the business's 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 young people 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.

All staff will use a password manager to help them store their passwords securely. Trainers will generate passwords for young people using a password manager/generator and keep these in a secure location in case young people lose or forget their passwords.

Our business will allocate passwords to staff and will require regular password updates. This will be done by ICT manager.

### 8.2 Software updates, firewalls, and anti-virus software

All the business's ICT devices that support software updates, security updates and anti-virus products will 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 business's ICT facilities.

Any personal devices using the business's 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 business's data protection policy.

See website for our business's data protection policy.

### 8.4 Access to facilities and materials

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

These access rights are managed by the ICT manager.

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 ICT 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 closed down completely at the end of each working day.

### 8.5 Encryption

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

Business 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 Directors.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT manager.

## 9. Protection from cyber attacks

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

The business will:

- Work with employers and the IT department 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 business'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.
- Put controls in place that are:
  - **'Proportionate'**: the business will verify this using a third-party audit (such as [this one](#)) annually to objectively test that what it has in place is up to scratch.
  - **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 up to scratch and secure as they can be.
- Back up critical data regularly and ideally at least once a day (automatic)] and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the business network and which can be stored off the business premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider/our ICT manager.
- 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 seeing if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department, for example, including how the business will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- Work with our LA/trust to see what it can offer the business regarding cyber security, such as advice on which service providers to use or assistance with procurement.

## 10. Internet access

The business wireless internet connection is secured.

- We will use filtering (as advised by ICT manager and report any inappropriate and appropriate sites to ICT manager)
- We will have separate connections for staff/young people/parents/the public.

### 10.1 Young people

- Wi-Fi is available in the classroom.
- We will use filtering such as Smooth wall or use recommendations from our ICT manager.
- The young people can request access (ICT manager will decide how)
- The use of Wi-Fi is limited to research and Careers (application forms, looking for jobs etc)

### 10.2 Parents, visitors and students

Parents and students will not be permitted to use the business's Wi-Fi unless specific authorisation is granted by the Directors.

The Directors will only grant authorisation if:

- Parents are working with the business in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the business's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

## 11. Monitoring and review

The Directors and ICT manager will 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.

The Director board is responsible for approving this policy.

## 12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Mobile phone usage

We are not including a Remote Access Policy – we as a business will try our hardest to provide live teaching in the event of a lockdown, we will aim to offer an alternative session – if the school has immersive technology we will send our workplace sessions for them to access. If schools do not have the VR technology – we will offer an ICT version. (This will not be virtual.)

## Appendix 1: Facebook cheat sheet for staff

**Don't 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 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 young people.
6. Don't use social media sites during business hours.
7. Don't make comments about your job, your colleagues, our business, or your young people 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) can find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or young people)

---

### Check your privacy settings.

- › Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, young people 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](https://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](https://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 young people and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the Directors 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 trainers at the business.
  - Young people 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 pupil 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	
<b>Name of parent/carers:</b>	
<b>Name of child:</b>	
<p>Online channels are an important way for parents/carers to communicate with, or about, our business. The business uses the following channels:</p> <ul style="list-style-type: none"><li>• Our official Facebook/linked in page.</li><li>• Email/text groups for parents (for business announcements and information)</li></ul>	
<p>When communicating with the business via official communication channels, or using private/independent channels to talk about the business, I will:</p> <ul style="list-style-type: none"><li>• Be respectful towards members of staff, and the business, always.</li><li>• Be respectful of other parents/carers and children.</li><li>• Direct any complaints or concerns through the business's official channels, so they can be dealt with in line with the business's complaints procedure.</li></ul> <p>I will not:</p> <ul style="list-style-type: none"><li>• Use private groups, the business's 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 if they aren't raised in an appropriate way.</li><li>• Use private groups, the business's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other young people. I will contact the business and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident.</li><li>• 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</li></ul>	
<b>Signed:</b>	<b>Date:</b>

### Appendix 3: Acceptable use agreement for older young people (16-24 years old)

#### Acceptable use of the business's ICT facilities and internet: agreement for young people and parents/carers

**Name of pupil:**

**When using the business's ICT facilities and accessing the internet in business, I will not:**

- Use them for a non-educational purpose.
- Use them without a trainer being present, or without a trainer's permission.
- Use them to break business rules.
- Access any inappropriate websites.
- Access social networking sites (unless my trainer 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 trainer.
- 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.
- Share my password with others or log in to the business's 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 business's ICT facilities and systems.

I will immediately let a trainer 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 business's ICT systems and internet responsibly.

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

**Signed (pupil):**

**Date:**

**Parent/carers agreement:** I agree that my child can use the business's ICT systems and internet when appropriately supervised by a member of business staff. I agree to the conditions set out above for young people using the business's ICT systems and internet, and for using personal electronic devices in business, and will make sure my child understands these.

**Signed (parent/carers):**

**Date:**



## Appendix 4: Acceptable use agreement for younger young people (12-16 years old)

### Acceptable use of the business's ICT facilities and internet: agreement for young people and parents/carers

**Name of pupil:**

**When I use the business's ICT facilities (like computers and equipment) and get on the internet in business, I will not:**

- Use them without asking a trainer first, or without a trainer in the room with me.
- Use them to break business rules.
- Go on any inappropriate websites.
- Go on Facebook or other social networking sites (unless my trainer said I could as part of a lesson)
- Use chat rooms.
- Open any attachments in emails, or click any links in emails, without checking with a trainer first.
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes.
- Share my password with others or log in using someone else's name or password.
- Bully other people.

I understand that the business will check the websites I visit and how I use the business's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a trainer or a member of staff I know immediately if I find anything on a business computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the business's ICT systems and internet.

I understand that the business can discipline me 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 business's ICT systems and internet when appropriately supervised by a member of business staff. I agree to the conditions set out above for young people using the business's 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, employers, volunteers and visitors

### Acceptable use of the business's ICT facilities and the internet: agreement for staff, employers, volunteers and visitors

**Name of staff member/governor/volunteer/visitor:**

When using the business's 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 business'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 the business's network.
- Share my password with others or log in to the business's network using someone else's details.
- Share confidential information about the business, its young people 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 the business

I understand that the business will monitor the websites I visit and my use of the business'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 business, and keep all data securely stored in accordance with this policy and the business's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT 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 business's ICT systems and internet responsibly and ensure that young people in my care do so too.

**Signed (staff member/trustee/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 Business (NCSC) [glossary](#).

TERM	DEFINITION
<b>Antivirus</b>	Software designed to detect, stop and remove malicious software and viruses.
<b>Cloud</b>	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
<b>Cyber attack</b>	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
<b>Cyber incident</b>	Where the security of your system or service has been breached.
<b>Cyber security</b>	The protection of your devices, services and networks (and the information they contain) from theft or damage.
<b>Download attack</b>	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
<b>Firewall</b>	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
<b>Hacker</b>	Someone with some computer skills who uses them to break into computers, systems and networks.
<b>Malware</b>	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
<b>Patching</b>	Updating firmware or software to improve security and/or enhance functionality.
<b>Pentest</b>	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
<b>Phishing</b>	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
<b>Ransomware</b>	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
<b>Social engineering</b>	Manipulating people into giving information or carrying out specific actions that an attacker can use.
<b>Spear-phishing</b>	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.
<b>Trojan</b>	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
<b>Two-factor/multi-factor authentication</b>	Using 2 or more different components to verify a user's identity.
<b>Virus</b>	Programs designed to self-replicate and infect legitimate software programs or systems.
<b>Virtual Private Network (VPN)</b>	An encrypted network which allows remote users to connect securely.
<b>Whaling</b>	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.