

REBUILD • REINTEGRATE • REDISCOVER



# **ICT and ACCEPTABLE USE POLICY 2024/2025**



## ICT & ACCEPTABLE USE POLICY

Person responsible for this policy:	Paul Arch
Policy author:	Paul Arch
Date Approved by Directors:	January 2024
Date to be Reviewed:	January 2026
Policy displayed on website:	Yes

CEO's Signatures:	Paul Arch Viv Hunt
-------------------	-----------------------

Updates made:	Date:

## 1. Scope

ICT is an integral part of the way Reboot Education works, and is a critical resource for pupils, staff and visitors. It supports teaching and learning, pastoral and administrative functions of Reboot Education.

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

This policy aims to:

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

This policy covers all users of Reboot Education's ICT facilities, including staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Disciplinary Policy.

## 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 2018](#)
- [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, 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 Reboot Education to use the 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.
- "Authorised personnel": employees authorised by Reboot Education 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 Reboot Education's ICT facilities by any member of Reboot Education's community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of Reboot Education's ICT facilities includes:

- Using Reboot Education's ICT facilities to breach intellectual property rights or copyright.
- Using Reboot Education's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching Reboot Education'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 Reboot Education, or risks bringing the company into disrepute.
- Sharing confidential information about Reboot Education, its pupils, staff or other members of Reboot Education's community.
- Connecting any device to Reboot Education's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on Reboot Education'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 Reboot Education'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 Reboot Education.
- Using websites or mechanisms to bypass Reboot Education's filtering mechanisms.

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

### 4.1 Exceptions from unacceptable use

Where the use of Reboot Education ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the discretion of the Directors at Reboot Education.

Staff should consult the Directors of Reboot Education, on how and why they intend to use Reboot Education's IT facilities. If permission is given, the decision will be recorded and kept on electronic file.

### 4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with Reboot Education's policies on Behaviour, Staff Code of Conduct or Staff Discipline.

## **5. Staff (including volunteers, and contractors)**

### **5.1 Access to academy trust ICT facilities and materials**

The Director of Education, along with Technical Support, will manage access to Reboot Education ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing Reboot Education'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 Director of Education.

#### **5.1.1 Use of phones and email**

Reboot Education provides each member of staff with an official email address which gives them access to the suite of Office tools on Microsoft 365.

This email and office account should be used for work purposes only.

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

Staff must not share their personal email addresses with parents 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 Reboot Education's Data Protection Lead and 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 Reboot Education's Director of Education immediately and follow our data breach procedures (see Data Protection policy).

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by Reboot Education or Phone app to conduct all work-related business.

Reboot Education phones must not be used for personal matters unless permission has been given by the Reboot Education's Company Directors.

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.

Staff who would like to record a phone conversation for purposes other than professional development should speak to the Company Directors for authorisation. The parent will be informed that a call is being recorded.

Reboot Education's Directors 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.

## 5.2 Personal use

Staff are permitted to occasionally use Reboot Education ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Director of Education 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 the main work day.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils or parents are present.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

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

Staff are permitted to use their personal devices (such as mobile phones/ tablets or smart watches) to access Reboot Education related apps such as Microsoft 365, Purple Mash, as long as no confidential information is download/ screenshotted and saved on the device.

Staff should be aware that personal use of ICT (even when not using Reboot Education's ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them (see social media policy).

Staff should take care to follow Reboot Education'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 that their use of social media, either for work or personal purposes, is appropriate at all times.

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

## 5.3 Remote access

We allow technical staff to access Reboot Education's ICT facilities and materials remotely.

Reboot Education's Technical Support Manages this access.

Support use Team Viewer as their host.

Remote access is not granted to members of Reboot Education's staff beyond technical support.

Technical Support accessing Reboot Education's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. They must be particularly vigilant if they use Reboot Education's ICT facilities outside Reboot Education and take such precautions as may be required from time to time 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.

## **5.4 School social media accounts**

Reboot Education has an official X (formerly Twitter), Facebook and Instagram pages. These are managed the Company Directors. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Reboot Education 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.

For example, only children with adequate internet permissions may appear. Staff must not use their personal devices to take photographs of pupils to upload to social media.

## **5.5 Monitoring of school network and use of ICT facilities**

Reboot Education 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.

Reboot Education monitors ICT use in order to:

- Obtain information related to Reboot Education business.
- Investigate compliance with Reboot Education's policies, procedures and standards.
- Ensure effective Reboot Education 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. Pupils

### 6.1 Access to ICT facilities

Reboot Education Computers and equipment are available to pupils only under the supervision of staff.

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

All pupils are provided with a login for the network. Children are also given accounts for other software such as Purple Mash.

Passwords are unique to each child. Children are regularly reminded not to share their passwords with anyone else.

### 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](#), Reboot Education has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under Reboot Education's rules or legislation.

Reboot Education 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 Reboot Education's rules.

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

Reboot Education will sanction pupils, in line with our Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on Reboot Education 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 Reboot Education'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 Reboot Education, or risks bringing Reboot Education into disrepute.
- Sharing confidential information about Reboot Education, other pupils and staff.
- 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 Reboot Education'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.

## **7. Parents**

### **7.1 Access to ICT facilities and materials**

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

### **7.2 Communicating with or about the school online**

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


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

We ask parents to sign the agreement in appendix 2.

## **8. Data security**

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

### **8.1 Passwords**

All users of Reboot Education's ICT facilities should set strong passwords for their accounts and keep these passwords secure and not share with anyone else. 

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

Pupils have their passwords for software like Purple Mash randomly generated.

Members of staff or pupils 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.

Staff should update their passwords at least every six months using a combination of: Upper case letters, lower case letters, numbers and symbols. Passwords must be at least eight characters long.

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

All of Reboot Education'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 Reboot Education's ICT facilities.

Any personal devices using Reboot Education'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 Reboot Education's data protection policy.

## **8.4 Access to facilities and materials**

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

These access rights are managed by our IT technicians and the Director of Education.

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 CEOs of Reboot Education 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**

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

Reboot Education staff may only use personal devices (including computers and USB drives) to access Reboot Education data, work remotely, or take personal data (such as pupil information) off site, if they have been specifically authorised to do so by the company's CEOs.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by Reboot Education's Technical Support or company CEOs.

Reboot Education staff may only use Cloud Based Storage services that have been provided by Reboot Education (such as Microsoft 365) to store Reboot Education data and personal data as these systems have encryption and password security at the approved level.

## **9. Internet access**

Wireless internet connections are securely filtered and the access code updated every six months.

Filtering is not fool-proof. If staff, parents, visitors or pupils identify that inappropriate content is being or could be viewed, they must inform Reboot Education's CEOs immediately so that the filters can be updated.

If staff are using Reboot Education ICT equipment at home, it is advisable that they change the default usernames and passwords for their home wi-fi router, as these are often publicly available on the Internet and can leave Reboot Education ICT equipment vulnerable to hackers, who could access files and introducing viruses and malware.

### **9.1 Pupils**

Pupils can only access the internet under the supervision of a member of Reboot Education staff.

### **9.2 Parents and visitors**

Parents and visitors to Reboot Education will not be permitted to use Reboot Education's secure wi-fi network. However, they may be given access to Reboot Education's 'guest' wi-fi network, which is unsecure.

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

## **10. Monitoring and review**

Reboot Education's CEOs in collaboration with Reboot Education's technical support monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of Reboot Education.

This policy will be reviewed every two years.

Reboot Education's CEOs are responsible for approving this.

## 11. Related policies

This policy should be read alongside Reboot Education's policies on:

- Online safety
- Safeguarding
- Behaviour
- Staff discipline/Code of Conduct
- Data protection/GDPR

## Appendix 1: Social Media cheat sheet for Reboot Education's staff

### Don't accept friend requests from pupils on social media

#### 10 rules for Reboot Education staff on social media.

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 pupils
6. Don't use social media sites during hours when pupils are on site.
7. Don't make comments about your job, your colleagues, Reboot Education or your pupils online - once it's out there, it's out there.
8. Don't associate yourself with Reboot Education on your profile (e.g. by setting it as your workplace, or by 'checking in' at a work 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 wi-fi connections and makes friend suggestions based on who else uses the same wi-fi 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](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 do to 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 Reboot Education's CEOs and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify Reboot Education's CEOs 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 members of staff at Reboot Education.
- Pupils 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, Reboot Education's CEOs 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/carers:**

**Name of child:**

Online channels are an important way for parents/carers to communicate with, or about, Reboot Education. The school uses the following channels:

- Our official X (formerly Twitter) account
- Email/text groups for parents (for Reboot Education announcements and information)

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's education. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

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

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

I will not:

- Use private groups, Reboot Education's X (formerly Twitter) page, or personal social media to complain about or criticise members of staff. This is not constructive and Reboot Education can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, t Reboot Education's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact Reboot Education 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

**Signed:**

**Date:**

### Appendix 3: Acceptable use agreement for older pupils

#### Acceptable use of Reboot Education's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

**When using Reboot Education's ICT facilities and accessing the internet at Reboot Education, 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 Reboot Education 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 Reboot Education's network using someone else's details
- Bully other people

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

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

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:



## Appendix 4: Acceptable use agreement for younger pupils

### Acceptable use of Reboot Education's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

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

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break Reboot Education rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher 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 teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that Reboot Education will check the websites I visit and how I use Reboot Education'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 teacher or a member of staff I know immediately if I find anything on a Reboot Education computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use Reboot Education's ICT systems and internet.

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

Signed (pupil):

Date:

**Parent/carer agreement:** I agree that my child can use Reboot Education's ICT systems and internet when appropriately supervised by a member of Reboot Education staff. I agree to the conditions set out above for pupils using Reboot Education's ICT systems and internet, and for using personal electronic devices at Reboot Education, 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 Reboot Education's ICT facilities and the internet: agreement for staff, volunteers and visitors

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

When using Reboot Education's ICT facilities and accessing the internet at Reboot Education, or off site 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 Reboot Education'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 Reboot Education's network
- Share my password with others or log in to Reboot Education's network using someone else's details
- Share confidential information about Reboot Education, 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 private businesses, unless that business is directly related to Reboot Education.

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

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

I will let Reboot Education's CEOs and designated safeguarding lead (DSL) know if a pupil informs me that 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 Reboot Education's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/volunteer/visitor):**

**Date:**