

Albany Learning Trust

ICT and internet acceptable use policy

To be used by all academies in the Trust

Version	1
Name of Policy writer	Gill Smith
Last Updated	October 2020
Review Date	October 2023
Approved	
ICO registration number	

Contents

1. Contents	1
2. Relevant legislation and guidance.....	2
3. Definitions	2
4. Unacceptable use.....	2
5. Staff (including governors, members, trustees, volunteers, and contractors)	3
6. Pupils	5
7. Parents	6
8. Data security.....	6
9. Internet access	7
10. Monitoring and review	8
11. Related policies	8

1. Introduction and aims

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

However, the ICT resources and facilities that Trusts/academies within Albany Learning Trust use also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

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

Breaches of this policy may be dealt with under our staff code of conduct.

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 Trusts](#)

Copies of the Trust's GDPR privacy notice and safeguarding policy are available

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 Trust to use the ICT facilities, including governors, members, trustees, 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 the Trust 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 the Trust's ICT facilities by any member of the Trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's ICT facilities includes:

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

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

4.1 Exceptions from unacceptable use

Where the use of Trust ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's/Head of School's discretion. To obtain approval for such exemption written request must be made directly to the Headteacher/Head of School.

4.2 Sanctions

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

5. Staff (including governors, members, trustees, volunteers, and contractors)

5.1 Access to Trust ICT facilities and materials

The Trust's IT manager is responsible for ICT services manages access to the Trust's ICT facilities and materials for Trust 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 the Trust'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 The Trust's IT manager responsible for ICT services.

5.1.1 Use of phones and email

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

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the Trust 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 not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer/Miss Linda Burrows immediately and follow our data breach procedure.

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

Trust 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.

5.2 Personal use

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Trust's IT manager responsible for ICT services 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 pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust'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 Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's 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 Trust ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the Trust'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.

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

5.3 Remote access

Staff are able to access the Trust's ICT facilities and materials remotely. Microsoft Remote Desktop Services is used to connect to the Trust's data. The connection to the Remote Desktop Server or Sims application is encrypted and establishing through Remote Desktop Gateway server.

ICT services manage access to the Gateway Server and the Remote Desktop Server in Active Directory. The Remote Desktop usage is monitored and all staff accessing remote Desktop do so using network credentials.

Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the Trust and take such precautions as the Headteacher may require 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. This may be found in the public shared area in the staff folder under policy.

5.4 Trust social media accounts

The Trust has official Twitter 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 Trust 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.

5.5 Monitoring of Trust network and use of ICT facilities

The Trust 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

Monitoring software is actively used and provides alerts to key staff when inappropriate content is accessed and inappropriate language is used. Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The Trust monitors ICT use in order to:

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

6.1 Access to ICT facilities

- Computers and equipment in the Trust's ICT suite 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.

- Pupils will be provided with an account linked to the Trust’s virtual learning environment, Google classroom, which they can access from any device by using the following URL google.com.

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 Trust has the right to search pupils’ phones, computers or other devices for pornographic images or any other data or items banned under Trust rules or legislation.

The Trust 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 Trust’s rules.

6.3 Unacceptable use of ICT and the internet outside of Trust

The Trust will sanction pupils, in line with the student behaviour and discipline policy, if a pupil engages in any of the following **at any time** (even if they are not on Trust 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 Trust’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 the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, other pupils, or other members of the Trust 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 Trust’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 the Trust’s ICT facilities as a matter of course.

However, parents working for, or with, the Trust in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the Trust’s facilities at the Headteacher’s/Head of School’s discretion.

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

7.2 Communicating with or about the Trust 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 the Trust through our website and social media channels.

We ask parents to adhere to our cooperative interaction policy.

8. Data security

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

8.1 Passwords

All users of the Trust'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 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.

8.2 Software updates, firewalls, and anti-virus software

All of the Trust'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 Trust's ICT facilities.

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

8.4 Access to facilities and materials

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

These access rights are managed by the Trust's IT manager responsible for ICT services.

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 Trust's IT manager responsible for ICT services 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 Trust ensures that its devices and systems have an appropriate level of encryption.

Trust staff may only use personal devices (including computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of Trust if they have been specifically authorised to do so by the Headteacher/Head of School.

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

9. Internet access

The Trust wireless internet connection is secured. Staff and pupils are subject to different levels of filtering. Staff must be aware that filtering is not fool proof. Any inappropriate sites that the filter has not identified or appropriate sites that have been filtered in error, must be reported to ICT services or the the Trust's IT manager responsible for ICT services. Albany BYOD is the guest network and is subject to filtering. BYOD is password secured. Access to the BYOD wifi network is granted at the discretion of the Trust's IT manager responsible for ICT services.

9.1 Pupils

When using Trust's own mobile devices such as ipads, pupils are permitted to utilise the Trust wifi network. Pupils are not permitted to use their own devices on the Trust premises. Trust's own mobile devices are connected to BYOD wifi and pupils must be supervised when using these devices. Any misuse must be reported to the the Trust's IT manager

responsible for ICT services. Trust's mobile devices are set up ready for use by ICT services. Requests for the installation of apps must be made to ICT services.

9.2 Parents and visitors

Parents and visitors to the Trust will not be permitted to use the Trust's wifi unless specific authorisation is granted by the Headteacher/Head of School.

The Headteacher/Head of School will only grant authorisation if:

- Parents are working with the Trust in an official capacity (e.g. as a volunteer)
- Visitors need to access the Trust's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

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

10. Monitoring and review

The Headteacher /Head of School and the Trust's IT manager responsible for ICT services monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed every 3 years.

The governing board is responsible for approving this policy.

11. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection, information management and retention
- Cooperative interaction

APPENDIX 1: SOCIAL MEDIA CHEAT SHEET FOR STAFF

10 rules for Trust staff on Facebook and other social media

Don't accept friend requests from pupils 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 Trust hours
7. Don't make comments about your job, your colleagues, our Trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the Trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a Trust 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 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 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 Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the Trust
- 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, 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: GUIDANCE ON VIDEO CONFERENCING

What is video conferencing?

Video conferencing is a live audio and video conversation between 2 or more people in different locations, conducted using phone, tablet, laptop or desktop computer. Some video conferencing services also allow you to share files, pictures, or each other's screens.

Many devices have video conferencing functionality built in (such as Apple's FaceTime and Google's Duo), and many popular apps also provide this service (such as Instagram, WhatsApp and Facebook). There are also standalone video conferencing apps that you can download; popular titles include Zoom, Skype, Houseparty and Microsoft Teams.

Regardless of the type of service you use, this guidance is applicable to all video conferencing services. For more information about the security features of a specific service, please refer to the service providers' **official** support site.

Downloading video conferencing software

If you're downloading standalone video conferencing software, make sure that you firstly **check suitability with ICT services/Head Teacher/Head of School** and that you:

Only download the software from trusted sources. This means using your phone or tablet's app store (such as Apple's App Store or Google Play), or downloading the software from the service provider's **official** website. Be wary of following advertised links at the top of search results pages (they will typically include the word 'Ad' at the beginning of the address or description of the website), and adverts for video conferencing software within websites. These may contain links to sites that are not always legitimate, and can be used to scam people. You should also treat any unsolicited links you receive that refer to video conferencing software with caution.

Check online to understand what app is right for you. In most cases, the 'free' version of a video conferencing service will provide good enough functionality and security for personal use, provided you've set it up correctly. Premium versions of the same product may offer additional features and usability. You should consider paying for these versions if you feel you'd benefit from extra features. With so many products available, you may want to carry out your own research beforehand - using tech websites or other trusted sources - to find out which one is right for you.

Check the privacy settings. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.

Setting up video conferencing services

Before making your first call, you should:

Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password. If you need to install the video conferencing app, you'll have to create an account for it. Make sure that the password you use is different to all your other passwords, and difficult for someone to guess. You should also set up two factor authentication (2FA) for the account (and for your device and other apps if available), as this provides an extra layer of protection and can stop criminals accessing your accounts (even if they know your password).

Test the service before making (or joining) your first call. Most services have a 'test' function to ensure your microphone and camera work correctly, and that your internet connection is fast enough. You can also use the test function to learn how the service works. As a minimum, make sure you know how to mute your microphone and turn off the camera. This will give you more control over what you share with others.

Understand what features are available. Many services allow you to record the call, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded, what exactly is recorded (audio, pictures, messages), and who can access the recordings. There may also be additional controls to manage who can join the call.

Hosting and joining calls

It's important that you can control who can join your video conferencing call. For specific instructions, refer to the support website of the service you're using. However, the following general rules apply:





Do not make the calls public. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. For some video conferencing services, you can set up the call so that a password is required in order to join. This adds another layer of protection. Do not post the link (or the password) publicly.

Know who is joining your call. If you are organising the call for your family or friends consider using the lobby feature to ensure you know who has arrived. This is especially useful if individuals are joining the call via an unrecognised phone number. Make sure people are who they say they are before they join the call (the password function described above can help with this).

Consider your surroundings. Take a moment to think about what your camera shows when you're on a call. Would you want to share that information with strangers? Consider blurring or changing your background - you'll find instructions on how to do this on the support website for your video conferencing service.

Finally, make sure that **all** your devices and applications (not just the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to [protect yourself online](#). Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security.

EYFS Acceptable Use Policy Agreement

 <p>My Learning</p>	<ul style="list-style-type: none">• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.• I will ask a teacher before using a device and ask for help if I can't work the device.• I will only use activities that a teacher has told or allowed me to use.• I will ask a teacher if I am not sure what to do or I think I have done something wrong.• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 <p>My Online Safety</p>	<ul style="list-style-type: none">• I will always use what I have learned about Online Safety to keep myself safe.• I will tell a teacher if I see something that upsets me on the screen.
 <p>Using the Internet @school</p>	<ul style="list-style-type: none">• I will only use the internet when the teacher says I can.• I will only go on websites that my teacher allows me to.• I will tell my teacher if I go on a website by mistake.
 <p>Using the Internet @home</p>	<ul style="list-style-type: none">• I will tell a trusted adult if I see something that upsets me on the screen.

I understand that these rules help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

Child's Signature

Parents:

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.





I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent's Signature

Date

Year 1 and Year 2 Acceptable Use Policy Agreement

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 <p>My Online Safety</p>	<ul style="list-style-type: none"> • I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> • I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> • I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that these rules help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

Child's Signature

Parents:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.




I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent's Signature

Date

Year 3 and Year 4 Pupils School Acceptable Use Policy Agreement

 <p style="text-align: center;">My Learning</p>	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 <p style="text-align: center;">Using the Internet @school</p>	<ul style="list-style-type: none"> • I will only visit sites that are appropriate to my learning at the time <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may use it. <p>My role as a Digital Citizen.</p> <ul style="list-style-type: none"> • I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
 <p style="text-align: center;">Using the Internet @home</p>	<ul style="list-style-type: none"> • I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies eg: CEOP, Childnet, Childline, Barnardos <p>My Communications</p> <ul style="list-style-type: none"> • I will be aware of the "SMART" rules, when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use inappropriate language and I understand that others may have different opinions. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

Child's Signature

Parents:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.




I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent's Signature

Date

Year 5 and Year 6 Pupils Acceptable Use Policy Agreement

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> • I will only visit sites that are appropriate to my learning at the time <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may steal it. <p>My role as a Digital Citizen.</p> <ul style="list-style-type: none"> • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> • I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos. <p>My Communications (Including texting and messaging)</p> <ul style="list-style-type: none"> • I will be aware of "stranger danger", when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parent understand that keeping me safe on the internet at home is their responsibility.

Child's Signature

Parent:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent's Signature

Date