Bringing out the best in everyone

NCBIS

Since 1978 New Cairo British International School

Name of Policy:	Acceptable Use Policy
Applicable to:	Whole School
Written by:	Jennifer Surujpaul
Contributors:	SLT, HR, Finance, HODs
Approved on behalf of the ELT	John Bagust
Effective date:	June 2019
Date of next review:	June 2021

NCBIS Mission Statement:

To provide a learning environment that supports academic achievement whilst promoting personal growth through the attributes of the IB Learner profile, within a caring international community committed to the traditional values of honesty, courtesy, respect, integrity and fair play.

Purpose and Scope of Policy

NCBIS recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and board members will be able to use the internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers

Voluntary or community organisations using the school's facilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events such as parent workshops. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

Links to other relevant school policies and guidance notes:

- Anti-Bullying
- Bus Guidance for Parents and Pupils
- Safeguarding Children: Child Protection
- Online Safety
- Safeguarding Children: Voicing Concerns
- Acceptable Internet Use and Agreement
- Asset Management
- Health and Safety

- Mobile Phone Safety and Acceptable Use

Aims

- To ensure all school personnel read and sign the 'Equipment Loan Form'.
- To share good practice within the school and with other schools.
- To ensure compliance with all relevant legislation connected to this policy.
- To work with other schools to share good practice in order to improve this policy

Responsibility for the Policy and Procedure

Role of the Board of Directors

The Board of Directors has:

- appointed a Business Manager to be responsible for the security of school property;
- delegated powers and responsibilities to the Director of IT to ensure all school personnel are aware of and comply with this policy;
- responsibility for ensuring full compliance with all statutory responsibilities;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- nominated a link BOD to:
    - visit the school regularly;
    - work closely with the Principal and the Director of Finance;
    - ensure this policy and other linked policies are up to date;
    - ensure that everyone connected with the school is aware of this policy;
    - attend training related to this policy;
    - report to the BOD every term;
    - responsibility for the effective implementation, monitoring and evaluation of this policy.

Role of the Principal

The Principal will:

- ensure all school personnel comply with this policy;
- ensure good practice is shared throughout the school;
- work closely with the link Board of Directors and the Director of Finance;
- provide leadership and vision in respect of equality;
- make effective use of relevant research and information to improve this policy;
- provide guidance, support and training to all staff;
- make effective use of relevant research and information to improve this policy;
- monitor the effectiveness of this policy by speaking with school personnel;
- annually report to the Board of Directors on the success and development of this policy.

Role of the Director of Finance and Director of IT

The Director of Finance will:

- lead the development of this policy throughout the school;
- work closely with the Principal and the nominated Board of Director;
- be in charge of the asset management system
- ensure all laptop equipment is:
    - insured
    - under warranty

    - asset tagged
    - included in the school inventory
    - password protected
    - securely stored while on school premises
    - supplied with a protective laptop bag
    - installed with original licensed software such as:
        - Microsoft Windows
        - Microsoft Internet Explorer
        - Microsoft Office
        - Anti -Virus Software
    - covered by technical support
    - annually maintained
- ensure all personnel sign the 'Equipment Loan Agreement';
- provide guidance and support to all staff;
- provide training for all staff on induction and when the need arises regarding;
- make effective use of relevant research and information to improve this policy;
- keep up to date with new developments and resources;
- undertake risk assessments when required;
- review and monitor;
- annually report to the Board of Directors on the success and development of this policy.

Role of School Personnel

School personnel will:

- comply with all aspects of this policy;
- be aware of all other linked policies;
- sign the 'Equipment Loan Form' which covers all usage before they are issued with a school laptop;
- use their work equipment with respect on and off-site;
- ensure the security of school equipment when off-site;
- maintain high standards of ethics and behaviour within and outside school and not to undermine fundamental British values;
- implement the school's equalities policy and schemes;
- report and deal with all incidents of discrimination;
- attend appropriate training sessions on equality;
- report any concerns they have on any aspect of the school community.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the Staff Code of Conduct
- meetings with school personnel.

Contents

1. Introduction and aims

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

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

This policy aims to:

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

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

Breaches of this policy may be dealt with under:

- NCBIS Staff Code of Conduct
- NCBIS Behaviour Policy

Relevant legislation and guidance

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

- Keeping Children Safe in Education 2018

2. 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 school to use the ICT facilities, including Board of Directors, 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 school 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.

3. Unacceptable use

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

Unacceptable use of the school's ICT facilities includes:

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

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

4. Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the principal's discretion. This would require consultation with the IT Director to evaluate any potential threats to NCBIS network

and authorisation would be completed using signed form. E.G: Teachers requiring projectors outside school at external venue, since this may cause issues for the event if equipment breaks down for any reason, there should be someone to sign for exception and be responsible for this or laptops on loan outside school to students for emergencies.

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

5.1 Access to school ICT facilities and materials

- The school's Tech Support team manages access to the school's ICT facilities and materials for school 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 school'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 tech support via email techsupport@ncbis.co.uk. In case of emergency, staff should contact IT Director via email or phone.
- Staff will need to submit through ManageEngine to facilitate their requests though mailing the tech support on techsupport@ncbis.co.uk or opening a ticket over the portal of ManageEngine using mobile phones, laptops or desktops.

5.1.1 Use of phones and email

E-Mail Etiquette

- All users should use a school email (ncbis domain) for all official communication to ensure everyone is protected through the traceability of communication.
- Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address.
- Pupils may only use school approved accounts on the school system and only for educational purposes.
- Emails created or received as part of any school role will be subject to disclosure in response to a request for information by Senior Leaders.
- Users should not open emails or attachments from suspect sources and should report their receipt to Director of IT
- Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).
- To encourage a better work-life balance and to make staff think more carefully about the emails they are sending, the following guidance should be adhered to:
    - E-mails should not be sent between the hours of 6.30pm and 6.30am.
    - Any emails that arrive in staff inboxes within the curfew are to be treated as though they arrived at 6.30am.
    - In terms of replies to staff, parents and students, a 2 working days period is stated in the Code of Conduct
    - All staff are required to check their emails at least twice a day, as suggestion once before and once after school.
    - During holidays or prolonged periods of absence, staff should turn on their Out of Office Autoreply function through their email settings, informing people the period of absence and who they should contact in the meantime. Staff are not expected to check or respond to emails during the holidays.

    - Avoid “reply all” email responses as far as possible.
    - E-mails should be professional in tone, and used for work purposes only.
- 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.

5.2 Personal use

Staff are permitted to occasionally use school 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 IT 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 should be aware that the use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’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 school’s mobile phone/personal device/smart watch guidance.
- Staff should be aware that personal use of ICT (even when not using school 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 school’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 school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school’s ICT facilities and materials remotely. Staff accessing the school’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 school’s ICT facilities outside the school and take such precautions as the Tech Support Team 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.

5.4 School social media accounts

The school has an official Facebook and Twitter page, managed by Marketing, SMT and IT Department. Staff members who have not been authorised to manage, or post to the account, must not access, or attempt to access the account.

The school 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 school network and use of ICT facilities

The school 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 school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school 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 school'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 school's virtual learning environment.
- "KS4 and KS5 pupils can use their own computers and the school's facilities in library, IT Suite, in class independently for educational purposes only"

6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, online safety policy and safeguarding policy, if a pupil engages in any of the following **at any time** (even if they are not on school 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 school'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 school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school 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 school'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

This will link directly to the Behaviour Policy, depending on the incident this will be aligned with the levelled response.

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PG) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Principal'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 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 the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

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

8.1 Passwords

- All users of the school's ICT facilities should set strong passwords (containing letters, numbers and / or special characters) 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.
- If trying to enter the wrong password for more than three times, the system will block you from entering the system until one of the administrators remove the block.
- The expectation is that all stakeholders change their password once a term (3 times a year)

8.2 Software updates, firewalls, and anti-virus software

- All of the school'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 school's ICT facilities.
- Any personal devices using the school's network must all be configured in this way.

8.3 Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
- These access rights are managed by Director of IT, Principal and Heads of Schools
- 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 Director of IT 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 and closed down completely at the end of each working day.

8.4 Encryption

- The school ensures that its devices and systems have an appropriate level of encryption.
- School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Principal or relevant .
- Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT Manager.

9. Internet access

The school wireless internet connection is secured.

- Wi-fi: Meraki Cisco as our main content filtering for staff, students and visitors

9.1 Pupils

Explain your school's approach to the use of wifi by pupils, including:

- Wifi is available around school buildings , but it's weak coverage at some certain areas like field , some classrooms in Secondary buildings.
- Any security or filtering settings you use, In order to get access to the network you need to have access codes provided by IT, filtering settings like content filtering is already applied once you get access to a wifi network and filtering application is meraki cisco content filtering
- How pupils can request access , They have to email techsupport@ncbis.co.uk or contact IT staff member

9.2 Parents and visitors

- Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Director of IT, Principal, Executive Business Manager and Heads of School
- Access will be granted based on the following:
    - Parents are working with the school in an official capacity (e.g. PG group)

    - Visitors need to access the school'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.

10. Monitoring and review

- The Principal and IT Director will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.
- This policy will be reviewed yearly
- The Board of Directors is responsible for approving this policy.

11. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Code of Conduct

Appendix 1: Facebook Cheat Sheet for Staff Guidance

Don't accept friend requests from pupils on social media

10 rules for school 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 pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. 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 Principal 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 school
    - 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: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Our official Facebook page ● Email/text groups for parents (for school announcements and information) ● Our virtual learning platform ● Parents are expected to receive a response to an email within 2 business days Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, 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 the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: ● Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way ● Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident ● Not use staff's personal phone numbers to contact them about my child ● 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 Secondary Students

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

Appendix 4: Acceptable use agreement for KS1

Pupil Acceptable Use Agreement - KS1	
This is how I stay safe when I use computers: ● I will keep my passwords secret. ● I will only use the computer for things my teacher has told me to. ● I will make sure that all the messages I send are polite. ● I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen. ● I will not reply to any nasty message or anything that makes me feel uncomfortable. ● I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school). In school, I will only use my school email. ● I will only email people I know or who my teacher says it is okay to email. ● I will never agree to meet a stranger. ● I will not put photographs of myself online without asking a teacher. I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.	
Signed (pupil):	**Date:**
Parent/carer agreement: This Acceptable Use Policy is intended to ensure: • that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. • that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. **Parent / Carer Signature** As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my child as part of whole school commitment to e-Safety 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. I understand that my child'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 e-Safety.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for KS2

Pupil Acceptable Use Agreement - KS2	
This is how I stay safe when I use computers: ● I will only use the Internet and/or online tools when a trusted adult is present. ● I will not deliberately look for, save or send anything that could be unpleasant or nasty. ● I will not deliberately bring in inappropriate electronic materials from home. ● I will not deliberately look for, or access inappropriate websites. ● If I accidentally find anything inappropriate I will tell my teacher immediately. ● I will only communicate online with people a trusted adult has approved. ● I will make sure that all ICT contact with other children and adults is responsible, polite and sensible. ● I will not give out my own, or others' details such as names, phone numbers or home addresses. ● I will not tell other people my ICT passwords. ● I will only open/delete my own files. ● I will not attempt to download or install anything on to the school network without permission. ● I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe. I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.	
Signed (pupil):	**Date:**
Parent/carer agreement: This Acceptable Use Policy is intended to ensure: • that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. • that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. **Parent / Carer Signature** As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my child as part of whole school commitment to e-Safety 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. I understand that my child'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 e-Safety.	

Signed (parent/carer):	**Date:**

Appendix 6: Acceptable use agreement for staff, Board of Directors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school 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 school'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 school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, 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 the school	
I understand that the school will monitor the websites I visit and my use of the school'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 school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT Director 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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 7: Acceptable Use of School Laptops and School Laptop Loan Agreement

We believe it is essential that all school personnel are issued with a school laptop which can be used on and off-site in order to assist them in the performance of their role and responsibilities within this school. Laptops are issued on loan to school personnel but remain the property of the school and must be returned in an acceptable condition on termination of employment.

We have in place adequate insurance cover for all school property or equipment that is used on premises only in the result of crisis such as earthquake, fire, armed attacks. This does not cover IT equipment used outside the school in case of accidental damage.

We advise all school personnel to have in place appropriate security measures to protect their laptop from damage or theft at all times. When not in use the laptop must be locked away and not left unattended. School personnel must note that they are responsible for replacing the laptop if it is stolen from an unattended vehicle or if it is left unattended in their home for longer than 48 hours.

We will ensure that before a laptop is issued all school personnel read and sign the 'Equipment Loan Form'.

We recognise our responsibilities under the Health and Safety and will take all reasonably practicable steps to provide and maintain a safe and healthy working conditions (on the school premises and during school-sponsored activities), equipment and systems of work for all our pupils, school personnel and visitors to the school.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the coordinator, the Principal and the nominated Board of Directors.

A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the Governing Body for further discussion and endorsement.