Cramlington Village Primary School

ICT Policy for school and staff
(including Acceptable Use)

November 2022

“Empowering everyone to achieve”

Policy Title	ICT Policy (including Acceptable Use)
Policies that interrelate	Most Able Behaviour Management Policy Equality Policy and Equality Information and Objectives
Legal and Statutory documents linked	- Data Protection Act 2018 - The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 - Computer Misuse Act 1990 - Human Rights Act 1998 - The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - Education Act 2011 - Freedom of Information Act 2000 - Education and Inspections Act 2006 - Keeping Children Safe in Education 2022 - Searching, screening and confiscation: advice for schools 2022 - National Cyber Security Centre (NCSC): Cyber Security for Schools - Education and Training (Welfare of Children) Act 2021 - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people - Meeting digital and technology standards in schools and colleges
Governor Committee responsibility	Education
Date of last review	November 2022
Reviewer name and position	Sarah Koratzitis Vice Principal
Date of next review	November 2023
Date approved by Governors	22 Nov 2022
Audit file updated (date and name)	

Contents

1. Introduction and aims

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

We are committed to providing our children with the most effective, innovative, up to date technologies possible to support and enhance their learning, providing creative ways for them to learn and extend their knowledge beyond the classroom. We embrace technology and use it effectively in all aspects of our unique ethos. Our approach is not traditional. It is built around our desire to provide our children with the most effective resources possible. We understand and appreciate that we live in a rapidly changing world and as such we have invested in technology that we can adapt as these changes occur. We will continue to invest in technology where it supports learning for our children and enhances their experiences.

However, the ICT resources and facilities our school uses could 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 policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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 our disciplinary policy.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

ICT facilities: all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the school's ICT service

Users: anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

Authorised personnel: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

Materials: files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

4.1 Exceptions from unacceptable use

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

The staff member will need to make a request in writing to the Principal to obtain approval.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and disciplinary.

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

5.1 Access to school ICT facilities and materials

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

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Business Manager.

5.1.1 Use of phones and email

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

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

All work-related business should be conducted using the email address the school 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 that contains the personal information of another person, they must inform the School Business Manager and Principal immediately and follow our data breach procedure.

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

School 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.

Digital images - Staff should not use their personal phone, camera or any other devices with photograph/recording capabilities without permission e.g. for a school field trip. Phones should also not be used in school, they are to be locked within staff lockers provided for the duration of school (8:30-3:30). If personal equipment is being used for a school excursion it should be registered with the school and a clear undertaking that photographs will be transferred to the Google drive and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Digital images / video of pupils need to be stored securely on the Google Drive and old images deleted after a reasonable period, or when the pupil has left the school.

The school can record incoming and outgoing phone conversations.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so.

Staff who would like to record a phone conversation should speak to the Principal.

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

The principal 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 (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Principal may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during school hours
- 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 school'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 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 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 use of 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 make sure 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 School social media accounts

The school has an official Facebook and Twitter account, managed by the Business Manager and Principal. Staff members are allowed to post professional posts relating to the school and are not allowed to post personal messages. Staff members must abide by the Teaching standards at all times when posting on the school social media accounts.

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 may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.4 Monitoring and filtering of the school network and use of ICT facilities

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

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and Business Manager as appropriate.

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

The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the school's IT resource list (iPads, Chromebooks, desktop computers) are available to pupils only under the supervision of staff.

It will be ensured that equal opportunities in information and communication technology are addressed as follows:

- Pupils with special needs have equal access to the information and communication technology curriculum through the use of differentiated learning strategies and tasks. These are based on individual needs. More able pupils are planned for in line with our Gifted and Talented Policy. This is supported by our Equality policy.
- Specific teaching strategies are used to maximize access to the curriculum for pupils with EAL (English as an Additional Language)

- Gender equality is promoted by ensuring that both boys and girls have equal access to all aspects of the information and communication technology curriculum.

6.2 Search and deletion

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

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, you should proceed according to the behaviour policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the behaviour management policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Principal to decide on a suitable response. If there are images, data or files on the device that staff

reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Not copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour 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 making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

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 PTA) 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.

7.3 Communicating with parents about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks is shared.

In particular, staff will let parents know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

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

8.1 Passwords

All users of the school'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, visitors or volunteers who disclose account or password information may have their access rights revoked.

Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

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 have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school'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 school's data protection policy found here.

8.4 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 the Business Manager and Principal.

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 Business Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

9. Internet access

The school's wireless internet connection is secure and managed by KBR.

9.1. Pupils

Pupils can connect to the WiIFI on a school device (Chromebook, iPad etc). Pupils have to access the WIFI under supervision of a member of staff from the teaching team.

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 Principal.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school'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.

Appendix 1: Social media cheat sheet for staff

10 rules for school 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 you don't, 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. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Google your name to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this
- Remember that some information is always public: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify 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 but we strongly suggest not accepting the request. Bear in mind that:

- Responding to 1 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)** **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 unless they are 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** · **Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers**	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: **agreement for pupils and parents/carers**	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: · **Use them without asking a teacher first, or without a teacher in the room with me** · **Use them to break school 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** · **Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes** · **Share my password with others or log in using someone else's name or password** · **Bully other people** **I understand that the school will check the websites I visit and how I use the school'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 school computer or online that upsets me, or that I know is mean or wrong.** **I will always be responsible when I use the school's ICT systems and internet.** **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 school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, 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:

Staff Acceptable Use & Responsibilities Policy

1) Access

1.1 As a staff member at CVPS, I have access to a range of IT resources which can change from time to time depending on resource allocation.
1.2 An accredited, filtered Internet connection from any computer in school
1.3 A personal @villageprimary.org email account via gmail
1.4 Access to network printers.

2) E-Safety

2.1 I will regularly remind pupils of key e-safety messages such as 'never give out personal details online'.
2.2 I will report any accidental access to inappropriate material to my line manager
2.3 I will report any inappropriate websites to the ICT coordinator or my line manager
2.4 I will be vigilant when asking students to search for images
2.5 If a student accesses inappropriate material I will report it following the correct procedures
2.6 If I suspect a child protection issue I will report it following the correct procedures.
2.7 I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

3) Computer Security

3.1 I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (eg printers and projectors)
3.2 If I notice that ICT equipment or software is damaged or not working correctly, I will report it on the ICT Coordinator straight away
3.3 I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
3.4 I will always keep my user account credentials secure and not tell them to anyone else.

3.5 I understand that my staff logon gives me access to systems and information and I will not under any circumstances allow anyone else access to a computer under my logon credentials

3.6 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files. If I find that I do have access to an area that I know I should not have access to, I will inform the ICT Coordinator or the Principal immediately.

3.7 If I think someone else has obtained my login details, I will report it to the ICT Coordinator as soon as possible to get my login credentials changed

3.8 I will never knowingly bring a computer virus, spyware or malware into school.

3.9 If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this.

3.10 I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network

3.11 I will take care if I eat or drink whilst using ICT equipment

3.12 I will not reply to spam emails as this will result in more spam. Delete all spam emails.

3.13 If I lose or misplace any portable ICT equipment I will inform ICT Coordinator

3.14 I will not 'jailbreak' a school iPad, iPhone or iPod touch, Chromebook or any other school ICT equipment.

4) **Inappropriate Behaviour**

4.1 I will not store, download or distribute music, video or image files on my personal user space unless they are copyright free files related to school work

4.2 I will not send or post defamatory or malicious information about a person or about school on social media or other online media sites including news outlets

4.3 I will not post or send private information about another person

4.4 I understand that bullying of another person either by email, online or via text message will be treated with the highest severity

5) ICT Acceptable Use Policy for Staff

5.1 I will not use the internet for gambling

5.2 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people

5.3 If I am planning any activity which might risk breaking the ICT Acceptable Use Policy (eg research into terrorism for a legitimate project), I will inform the ICT Coordinator beforehand to gain permission.

5.4 If I mistakenly access material that is profane or obscene, I will inform my line manager immediately or I may be held responsible

5.5 I will not attempt to use proxy sites on the internet

5.6 I will not take a photo or video of a student or another member of staff without their permission

5.7 I will not load photos or videos of other staff and students to websites or social networking sites unless it is via the official school social networking sites (CVPS class Facebook pages and through the CVPS Twitter account) I will refer any instances of this to the Principal or Vice Principal.

6) Monitoring

6.1 I understand that all Internet and email usage will be logged and this information could be made available to my line manager on request
6.2 I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required with or without my permission
6.3 I will not assume that any email sent on the internet is secure. I will use the school email signature with disclaimer
6.4 I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without the person's knowledge.

7) Best Practice

7.1 I will not use school printing facilities to print none-work related materials.
7.2 I will only print out work that I need as a paper copy – where possible I will use school systems such as email to share information electronically.
7.3 I will report if a printer is not working or out of toner.
7.4 I understand that my @villageprimary.org e-mail is a work email account, and as such will be used for professional purposes.
7.5 I will only use the approved, secure @villageprimary.org email system for any school communication
7.6 I will only open attachments or download files from trusted sources
7.7 I will not view, download or distribute material that could be considered offensive or pornographic
7.8 I will obtain the school cameras to photograph and video trips and relevant events (I will not use my own cameras without prior arrangement).
7.9 I will upload photos and other materials to the photo account for the school on the villageprimary domain
7.10 I will save work regularly using sensible file names
7.11 I will organize my files in a sensible manner and tidy my user space and shared resource areas regularly
7.12 I will ensure that I regularly back up any work that is not saved using the school's Google Drive
7.13 I will observe health and safety guidelines where possible when using ICT equipment
7.14 I will not use my personal mobile during school hours, this will be locked safely in staff lockers provided.
7.15 I will read, sign and adhere to the CVPS IT Loan Agreement when I am provided with IT equipment for use in my role within CVPS

7) Data Protection

8.1 I will not share data protected information (including school images) with third party organisations without seeking advice first

8.2 If I am preparing a document that contains data protected information I will ensure that the document template I use has the appropriate protective marking (e.g. confidential, protectively marked).

8.3 I will ensure that I am aware of data protection issues and understand what is considered to be 'personal data'.

8.4 I will not display sensitive information or 'personal data' on a public display or projected image (e.g. a Smartboard or Prowise Screen).

8.5 I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave 'personal data' unprotected.

8.6 I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.

9) Social Networking

9.1 I will not communicate with students through my personal social networking sites .

9.2 I will ensure that any personal social networking accounts that I have are secure.

9.3 I will never create a social networking profile or account and use it for school purposes without prior authorisation from the Principal.

9.4 I will not send or post defamatory or malicious information about a person or about school on my personal social media or other online media sites.

9.5 I will never create a bogus social networking account or site that is associated with a member of staff, students or the school.

9.6 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, students or the school, I will inform the Principal immediately.

9.7 I will consider my professional status when communicating via my own social media sites where my connections are parents or friends of parents and my comments could negatively impact on the reputation of the school.

10) Sanctions

10.1 I understand that failure to comply with this Policy could lead to disciplinary action.

Signed: …….

Print Name: …….

Date: …….

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 manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.** **I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.**	
Signed (staff member/governor/volunteer/visitor):	**Date:**