LOVE God • LOVE Neighbour • LOVE Self

St Chad’s CofE Nursery and Infant School

Staff ICT and Electronic Devices Acceptable Use Policy

School Leader:	**K Gilsenan**	
Link Governor:	**A Repesa**	
Policy Approved	**Signed: P Geary**	**Date: 06.06.18**
Policy Reviewed	Signed: A Repesa	Date: 16.07.25
Policy Reviewed	Signed: M Scothbrook	Date: 17.11.21
Policy Reviewed	Signed: N Iqbal	Date: 01.10.20
Policy Reviewed	Signed: R Williams	Date: 19.06.19

Statement of intent

The Staff ICT and Electronic Devices Acceptable Use Policy has been designed to outline all responsibilities when using technology both on and off site, using personal and school devices and applies to all staff, volunteers, contractors and visitors.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following school policies:

- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images consent
- Data and Cyber-security Breach Prevention and Management Plan
- Finance Policy

This policy is divided into the following three sections:

- Acceptable Use
- Internet policy and code of practice
- Email policy and code of practice

Introduction

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from malware, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Acceptable Use

- The school has well-developed and advanced ICT systems, which it intends for you to benefit from.
- This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

This policy applies to any computer or other device connected to the school's network and computers. The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.
- Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.
- Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.
- Any member of staff found to have breached the school's Data Protection Policy or relevant legislation will face disciplinary action.
- Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.
- Since ICT facilities are also used by pupils, the school will have a Pupil E-safety acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.
- Pupils found to have been misusing the ICT facilities will be reported via MyConcern to the DSL
- School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.
Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files (over 500MB) without permission from the ICT technician.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Take their allocated classroom mobile phone out of the school premises, unless permitted by the headteacher.
- All data will be stored appropriately in accordance with the school's Data Protection Policy.
- Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.
- School-owned electronic devices will not be used to access personal social media accounts.
- Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.
- Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.
- Copyrighted material will not be downloaded or distributed.
- School-owned devices will be taken home for work purposes only, once approval has been sought from the headteacher and ICT lead. Remote access to the school network will be given to staff using these devices at home.
- School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.
- While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.
- Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.
- Use of a school-owned phone for personal use will be permitted for necessary calls lasting less than **10 minutes**. A charge may be requested as a result of calls exceeding this time.
- Should staff need to use the telephones for longer than this, authorisation will be sought from the headteacher. This authorisation will be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, staff will notify the headteacher after the call.
- Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.
- Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.
- Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.
- Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

Code of practice

The school's philosophy	In using ICT, you will follow the school's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.

Times of access	The network is available during term time. Out of term time the network may be subject to maintenance downtime and so may not be available for brief periods. You will be notified of any changes.
User ID and password and logging on	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be a mix of the following: • Contain at least six characters • A mixture of lower case and capital letters • At least one numbers • At least one symbol If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records and senior ICT staff monitor your use of the system. Use of the school's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse. You must not log on to more than one computer at the same time.
Printing	The school may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources.
Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the system	You must not connect any hardware which may be detrimental to the school's network.

Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff. You may use the encrypted USB memory sticks, or other portable storage media where a port is provided on the front of the computers. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Virus	If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the school's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. If you believe that you have a real need for additional space, please discuss this with a senior member of the ICT support staff. Read through files annually saved on the main server. Achieve or delete files that are no longer needed to save space.
Transferring files	You may transfer files to and from your network home directories using and encrypted USB/removable devices. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.
Reporting faults and malfunctions	You must report any faults or malfunctions by email to Mercury Helpdesk (Autotask) helpdesk@mercuryavs-ltd.co.uk, including full details and all error messages, as soon as possible.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, near school ICT equipment. You must always maintain a clean and quiet working environment.
Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.
Copies of important work	It is your responsibility to keep all work saved on the main server. Work is backed up remotely and saved for a limited time. Please contact the ICT lead as soon as possible, if any work is missing or lost on the school system. Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location.

Using school equipment off site	All equipment must be signed out before leaving the school premises: IPads: sign out sheet on top of the IPad trolley. Please note the IPad number displayed on the back of the IPad Long term use of school surfaces or laptops are logged by mercury • Data is collected, processed, transported, and used in accordance with the school's DDAT Data Protection Policy. • The staff members who are taking data from the school to fulfil their roles at home take full responsibility for the security of the data. • Staff members are advised to ensure that they have their own domestic insurance policies in places for household contents and buildings. • All electronic devices used in transferring data between the school and staff members' homes are password-protected to secure information in case of theft. • Staff members are not permitted to let their family members or friends use any school equipment.

Online safety policy and code of practice

- The school can provide access to the internet from desktop PCs/surfaces/laptops via the computer network and through a variety of electronic devices connected wirelessly to the network.
- Whenever accessing the internet using the schools or personal equipment you must observe the code of practice below.
- This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the school's facilities and information being damaged.
- Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.
- The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

Why is internet access available?
The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

Why is a code of practice necessary?
There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.

- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from the ICT lead.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect to protect the staff and pupils who access to the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the school's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

Code of practice

Use of the internet	The Internet should not be used for private or leisure purposes. It is provided primarily for education or business use.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Giving out information	You must not give any personal information concerning the school, children or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school's name and your name when accessing a service which the school subscribes to.
Personal safety	You should take care with who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet.
Hardware and software	You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the school are an important part of the school security arrangements and making any changes, however

	innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

Portable equipment

- All data on school-owned equipment will be synchronised with the school server and backed up once per month.
- Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked in location when they are not in use.
- Portable equipment will be transported in its protective case, if supplied.
- Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.
- When using classroom mobile phones, the ICT coordinator, headteacher, DSL and the DPO will assess and ensure that the necessary software is in place to meet data protection and safeguarding requirements.
- Parents will be discouraged from calling the phones. In emergencies, parents will contact school's contact number, not the classroom phone. Parents will be permitted to text the number for justified reasons, such as being late to collect a child at the end of the day.

Personal devices

- Staff members will use personal devices in line with the school's Data and Cyber-security Breach Prevention and Management Plan.
- All personal devices that are used to access the school's online portal, systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the headteacher before use and submitted for the routine checks outlined in Safety and security section of this policy.
- Staff using their own devices will sign an agreement stating that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by the ICT lead. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.
- Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.
- Members of staff will not contact pupils or parents using their personal devices.
- Personal devices will only be used for off-site educational purposes when mutually agreed with the headteacher.
- Inappropriate messages will not be sent to any member of the school community.
- Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

- Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.
- During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in location.

Removable media

Only recommended removable media will be used including, but not limited to, the following:

- USB drives
- DVDs
- CDs

- All removable media will be securely stored location when not in use. Staff will be required to sign removable media devices in and out when they use them.
- Personal and confidential information will not be stored on any removable media.
- The ICT lead will encrypt all removable media with appropriate security measures.
- Removable media will be disposed of securely by the ICT lead.

Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

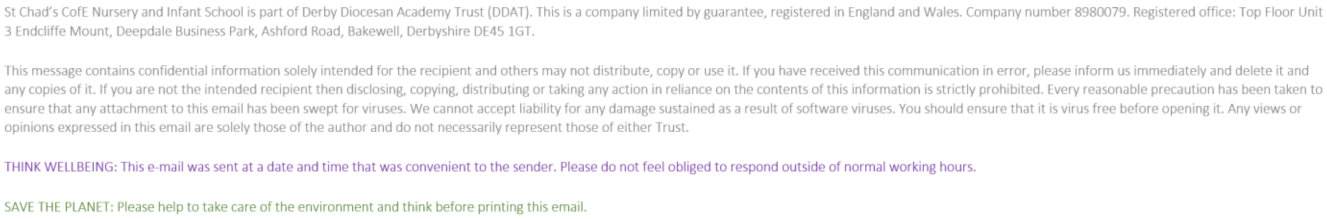
Storing messages

- Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of after no more than six months.
- Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.
- If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT lead.
- Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the headteacher, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

Email policy and code of practice

- The school email system and internet connection are available for communication and use on matters directly concerned with school business.
- Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.
- Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.
- Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

- If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.
- The school will be liable for any defamatory information circulated either within the school or to external contacts.
- The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.
- All emails that are sent or received will be retained within the school for a period of **six months** dependent on the information contained. More information can be found in the Record Retention Policy. The timeframe will be altered where an inbox becomes full.
- All emails being sent to external recipients will contain the school standard confidentiality notice. That notice will consist of:



St Chad's CofE Nursery and Infant School is part of Derby Diocesan Academy Trust (DDAT). This is a company limited by guarantee, registered in England and Wales. Company number 8980079. Registered office: Top Floor Unit 3 Endcliffe Mount, Deepdale Business Park, Ashford Road, Bakewell, Derbyshire DE45 1GT.

This message contains confidential information solely intended for the recipient and others may not distribute, copy or use it. If you have received this communication in error, please inform us immediately and delete it and any copies of it. If you are not the intended recipient then disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Every reasonable precaution has been taken to ensure that any attachment to this email has been swept for viruses. We cannot accept liability for any damage sustained as a result of software viruses. You should ensure that it is virus free before opening it. Any views or opinions expressed in this email are solely those of the author and do not necessarily represent those of either Trust.

THINK WELLBEING: This e-mail was sent at a date and time that was convenient to the sender. Please do not feel obliged to respond outside of normal working hours.

SAVE THE PLANET: Please help to take care of the environment and think before printing this email.

- Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the ICT technician. Staff will ensure that access to personal emails never interferes with work duties.
- Staff linking work email accounts to personal devices are permitted.
- The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.
- Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.
- Purchases for school equipment will only be permitted to be made online with the permission of the headteacher, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the SBM. This is in addition to any purchasing arrangement followed according to the school's Finance Policy.
- Any suspicious emails will be recorded in the incident log and will be reported to the headteacher. All incidents will be responded to in accordance with the Online Safety Policy.

Code of practice

Purpose	You should only use the school's email system for work related emails. You are only permitted to send a reasonable number of emails.

Trust's disclaimer	The school's email disclaimer is automatically attached to all outgoing emails and you must not cancel or disapply it.
Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email.
Program files and non-business documents	You must not introduce programme files or non-business documents from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the school. If you have any reason for suspecting that a virus may have entered the school's system, you must contact the ICT support staff immediately.
Quality	Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications. Staff members should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties • The emails sent and received may have to be disclosed in legal proceedings • The emails sent and received maybe have to be disclosed as part of fulfilling an SAR • Whether any authorisation is required before sending • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter • The confidentiality between sender and recipient • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.

	You must not send personal or inappropriate information by email about yourself, other members of staff, pupils or other members of the school community. If you receive any inappropriate emails or attachments, you must report them to ICT support and/or DSL.
Viruses	If you suspect that an email has a virus attached to it, you must inform the ICT support staff immediately.
Spam	You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff.
Storage	Old emails may be deleted from the school's server after 12 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep.
Message size	Staff are limited to sending messages with attachments which are up to 10Mb in size. If you wish to distribute files within the school, you can do so by using the shared server.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

Email policy – advice to staff

- Staff should check their emails every working day and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

Further guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.

- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT lead or headteacher. Certain items are asset registered and security marked; their location is recorded by the SBM for accountability. Once items are moved after authorisation, staff will be responsible for notifying the SBM of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed every six months. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the ICT lead or the headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the ICT technician or headteacher. This is in addition to any purchasing arrangements followed according to the Finance Policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.

- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance Policy.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the headteacher. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.
If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the headteacher.

Loaning electronic devices

- School equipment, including electronic devices, will be loaned to staff members.
- Loans will be requested by the ICT lead and must give at least three working days' notice prior to the requested loan date.
- Equipment and devices will only be loaned to staff members who have read, signed and returned the terms of use.
- By loaning school equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use.
- Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.
- The maximum loan period will be five working days; however, where required, this can be extended following discussion with the DEL and headteacher.
- If the equipment or device is no longer required, staff members will return the equipment to the DEL as soon as possible, allowing the equipment to be made available to someone else.

- Devices allowed for loan will be encrypted and protected to ensure the security of any data they hold.

Purchasing

- Funding for electronic devices, predetermined by the governing board, will be available each year on request from the SBM.
- Requests for equipment or electronic devices will be made via email to the SBM.
- Requests will be submitted in sufficient detail for an informed decision to be made.
- Requests will be responded to within three working days. If sufficient detail is not provided or other conditions specified by the SBM are not met, the request will not be processed.
- Requests made for equipment or electronic devices that exceed the predetermined amount allocated will require discussion and authorisation by the governing board.
- Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf unless permission has been sought from the headteacher.
- The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the headteacher.
- In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.
- The SBM will seek advice from the ICT lead and professionals when purchasing equipment.
- All equipment and electronic devices will be sourced from a reputable supplier (mercury).
- The SBM will maintain a Fixed Asset Register which will be used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.
- When devices are not fit for purpose, or are at least four years old, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the SBM, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear by the ICT technician.

Safety and security

- The school's network will be secured using firewalls in line with the Data and Cyber-security Breach Prevention and Management Plan.
- Filtering of websites, as detailed in the Data and Cyber-security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.
- Approved anti-virus software and malware protection will be used on all approved devices and will be updated on a termly basis.
- The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on a termly basis.
- Members of staff will ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, on a termly basis.
- Approved personal devices will also be submitted on a termly basis, to the ICT lead, so that appropriate security and software updates can be installed to prevent any loss of data. Consent

for such access will be obtained before the approval of a device – if consent if refused, the school reserves the right to decline a request to use a personal device.

- Records will be kept detailing the date and time, owner of a device and device type, on which the routine checks have taken place – these will be stored in location.
- Programmes and software will not be installed on school-owned electronic devices without permission from the ICT lead.
- Staff will not be permitted to remove any software from a school-owned electronic device without permission from the ICT lead.
- Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the ICT lead, may be subject to disciplinary measures.
- All devices will be secured by a password or biometric access control.
- Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.
- Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 10 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.
- All devices must be encrypted using a method approved by the DPO.
- Further security arrangements are outlined in the Data and Cyber-security Breach Prevention and Management Plan.

Loss, theft and damage

For the purpose of this policy, "damage" is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

- The school's insurance will cover school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises.
- Staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.
- Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.
- The ICT lead and headteacher will decide whether a device has been damaged due to the actions described above.
- The ICT lead will be contacted if a school-owned electronic device has a technical fault.
- If it is decided that a member of staff is liable for the damage, they will be required to pay 20 percent of the total repair or replacement cost. A written request for payment will be submitted to the member of staff who is liable to pay for damages.
- If the member of staff believes that the request is unfair, they can make an appeal to the headteacher, who will make a final decision within two weeks.
- In cases where the headteacher decides that it is fair to seek payment for damages, the member of staff will be required to make the payment within six weeks of receiving the request.

- Payments will be made to the SBM via the main office, and a receipt is given to the member of staff.
- The school will accept payments made via credit and debit cards, cheques and cash.
- A record of the payment will be made and stored in the main office for future reference.
- The headteacher may accept the payment in instalments.
- If the payment has not been made after six weeks, the fee will increase by five percent and continues for a maximum of six months – at which point formal disciplinary procedures will begin.
- The member of staff will not be permitted to access school-owned electronic devices until the payment has been made.
- In cases where a member of staff repeatedly damages school-owned electronic devices, the headteacher may decide to permanently exclude the member of staff from accessing devices.
- If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies.
- The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

Implementation

- Staff will report any breach of this policy to the headteacher.
- Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.
- Use of the telephone system will be logged and monitored.
- Use of the school internet connection will be recorded and monitored.
- The SBM will conduct random checks of asset registered and security marked items.
- Computer logs on the school network information is stored by mercury.
- Unsuccessful and successful log-ons will be logged on every computer connected to the school's network.
- Unsuccessful and successful software installations, security changes and items sent to the printer will also be logged.
- Mercury remotely view or interact with any of the computers on the school's network. This may be used randomly to implement this policy and to assist in any difficulties.
- The school's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.
- The school's database systems are computerised. Unless given permission by the ICT lead, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.
- All users of the database system will be issued with a unique individual password, which will be changed every six months. Staff will not, under any circumstances, disclose this password to any other person.
- Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.
- User accounts will be accessible by the headteacher and the ICT lead.
- Users will ensure that critical information is not stored solely within the school's computer system. Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.
Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

For further information or to clarify any of the points raised in this policy please speak to the DPO.

Appendix 1 – Staff ICT and Electronic Devices Acceptable Use Agreement

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The school may undertake monitoring activities of employees to ensure the quality and quantity of work. The school will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the school will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as unintrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. The school understands rights and the private lives of workers, particularly as remote working excessive monitoring can have adverse impacts continues to become more common, that excessive monitoring can have adverse impacts on data protection rights and the private lives of workers, particularly as remote working continues to become more common.

The school will ensure that the monitoring of workers is necessary for the identified reasons. The school will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's Data Protection Policy and any other relevant school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.

- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Follow the Staff ICT and Electronic Devices Policy.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the headteacher or ICT lead.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the headteacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the ICT lead.

- Seek permission from the headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the ICT lead.
- Immediately report any security issues, such as downloading a virus, to the ICT lead.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the ICT lead upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher.
- Install any software onto school-owned devices unless instructed to do so by the headteacher or ICT lead.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the headteacher or ICT lead.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the headteacher.

Social media and online professionalism

I will:

- Follow the school's Social Media Policy.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:

- Ensure I obtain permission from the headteacher and DPO before any personal data is transferred from a school-owned device to a personal device.
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure my personal device has been assessed for security by the DPO and ICT lead before it is used for home.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the ICT lead and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet will be monitored by mercury and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Monitoring workers

I understand that:

- The school will notify employees when monitoring takes place and that the school will clearly explain what personal information of mine is collected and how it's utilised and maintained.
- Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance.
- Monitoring technologies include, but aren't limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording.
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school.
- The school will factor in increased expectations of privacy if I work from home.
- The school will conduct its monitoring activities in a way that's fair and reasonably expected.
- The school will conduct its monitoring activities with transparency, clearly explaining how and why they process my information.
- The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR.
- I can object to having my personal information collected and processed if the lawful basis which the school is relying on is a public task or legitimate interests based on my personal situation.
- The school may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims.
- Tools for monitoring workers continue to become increasingly sophisticated, and that the school will inform me if they choose to use solely automated processes for monitoring activities.
- I can access the information collected by the school by making a subject access request (SAR).
- The school will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities.

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed (**staff member**): Date:

Print name:

Signed (**headteacher**): Date:

Print name:

Appendix 2

Loan Request Form
This form should be completed by staff members when requesting to loan school-owned equipment.

Staff members must detail the specific equipment or device which is requested, as well as provide a reason, and where necessary, evidence, as to why the equipment or device is required.

The completed form should be returned to the designated equipment lead (DEL) for authorisation.

Name		**Department**	
Equipment required			
Reason			
First date of loan		**Return date**	
Authorised (if rejected, detail why)			
Signed (DEL)			
Job role		**Date**	

Appendix 3

Purchase Request Form
This form should be completed by staff members when requesting for funds for the purchase of equipment or an electronic device.

Before submitting the form, any evidence supporting a purchase request or demonstrating the need for the equipment should be attached.

The completed form should be returned to the SBM for authorisation.

Name:		**Department**	
Purchase requested			
Amount required			
For use by			
Reason			
Supporting evidence			
How it will benefit pupils			
Authorised (if rejected, detail why)			
Signed			
Job role		**Date**	