

Robert Ogden School's ICT and Electronic Devices Policy

Version Number	1
Date of Issue / Latest Revision	March 2025
Guidance Lead(s)	Sara White - Safeguarding & Wellbeing Lead
Next Review	October 2026

Contents

Statement of intent.....	
Legal framework	
Roles and responsibilities.....	
Classifications.....	
Acceptable use.....	
Pupils acceptable use agreement.....	
Emails and the internet.....	
Portable equipment.....	
Personal devices.....	
Removeable media.....	
Cloud-based storage.....	
Storing messages.....	
Unauthorised use.....	
Loaning electronic devices.....	
Safety and security.....	
Loss, theft and damage.....	
Implementation.....	
Monitoring and review.....	

Appendices

Staff Declaration Form
 Loan Request Form
 Pupil Acceptable use Agreements
 Pupil Acceptable use Agreements (PECs)
 Letter to parents

Statement of intent

The Robert Ogden School believes that ICT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personal electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

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.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy and Online Safety Policy.

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:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Loaning School Equipment Policy
- Photography and Images Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Finance Policy
- Records Management Policy

Roles and responsibilities

The governing board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The headteacher is responsible for:

- Reviewing and amending this policy with the IT Co-Ordinator and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is carried out daily by the ICT Technician.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The IT Co-Ordinator or NAS ICT are responsible for:

- Carrying out checks on internet activity of user accounts and to report any inappropriate use to the headteacher.
- When concerns are raised they will monitor the computer logs on the school's network and to report any logged inappropriate use to the headteacher.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.
- Ensuring routine security checks are carried out on all school-owned laptops that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disabling user accounts of staff who do not follow this policy, at the request of the headteacher.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of devices to the DPO.
- The IT Co-Ordinator is responsible for the maintenance and day-to-day management of the equipment, as well as the device loans process.
- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance Policy.
- Overseeing purchase requests for electronic devices.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.

- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the headteacher or IT Co-Ordinator, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the headteacher or IT Co-Ordinator.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

Classifications

School-owned devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Camcorders
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

Acceptable use

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 and pupils 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 could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned 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 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 to the headteacher.

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.

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 IT Co-Ordinator.
- 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 and pupils 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 IT Co-Ordinator. Remote access 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.

More details about acceptable use can be found in the staff Technology Acceptable Use Agreement and Device User Agreement.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

Pupils acceptable use agreements

Our pupil agreement outlines the rules and guidelines for the acceptable use of technology and digital resources at The Robert Ogden School. It aims to protect students, staff, and the school community while promoting a safe and responsible digital environment.

This agreement applies to all pupils at The Robert Ogden School and covers all devices and digital resources provided by the school, including computers, tablets, internet access, and software.

The agreement is sent out annually to parents and carers and we request that they read the Acceptable Use Agreement with their child. Hopefully, this will also provide families with an opportunity for conversations between them and their child about safe and appropriate use of the technology, both at school and at home.

Emails and the internet

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 instance 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 Records Management Policy. The timeframe will be altered where an inbox becomes full.

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 IT Co-Ordinator. Staff will ensure that access to personal emails never interferes with work duties.

Staff linking work email accounts to personal devices, subject to the headteacher's approval.

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 monitored and recorded by the NAS ICT Team.

Portable equipment

All data on school-owned equipment will be synchronised with the school server and backed up.

Portable school-owned electronic devices should be locked when left unattended.

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.

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 when not in use.

Personal and confidential information will not be stored on any removable media.

The IT Co-Ordinator will encrypt all removable media with appropriate security measures.

Removable media will be disposed of securely by the IT Co-Ordinator.

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

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 IT Co-Ordinator.

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.

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 IT Co-Ordinator or headteacher. Certain items are asset registered and security marked; their location is recorded by the IT Co-Ordinator. Once items are moved after authorisation, staff will be responsible for notifying the IT Co-Ordinator of the new location.
- 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. 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 IT Co-Ordinator 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 IT Co-Ordinator or headteacher.

- 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 email to the IT Co-Ordinator who will then discuss with the head teacher.

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.

If the equipment or device is no longer required, staff members will return the equipment to the IT Co-Ordinator as soon as possible, allowing the equipment to be made available to someone else.

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 IT Co-Ordinator.

Approved anti-virus software and malware protection will be used on all approved devices.

The school will use mail security technology to detect and block any malware transmitted via email.

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.

Programmes and software will not be installed on school-owned electronic devices without permission from the IT Co-Ordinator.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the IT Co-Ordinator.

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the IT Co-Ordinator, 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.

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 IT Co-Ordinator
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

The IT Co-Ordinator and headteacher will decide whether a device has been damaged due to the actions described above.

The IT Co-Ordinator will be contacted if a school-owned electronic device has a technical fault.

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 school internet connection will be recorded and monitored.

The IT Co-Ordinator will conduct random checks of asset registered and security marked items.

The IT Co-Ordinator will check computer logs on the school network.

The IT Co-Ordinator may 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 IT Co-Ordinator, 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. 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 IT Co-Ordinator.

Users will ensure that critical information is not stored solely within the school's computer system.

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.

Monitoring and review

This policy will be reviewed annually by the IT Co-Ordinator and the headteacher.

Any changes or amendments to this policy will be communicated to all staff members by the headteacher.

Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.

By signing this form, you are declaring that you have read, understood and agree to the terms of the school's ICT and Electronic Devices Policy. You should read and sign the declaration below before returning it to the IT Co-Ordinator.

I have read the school's ICT and Electronic Devices Policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- The school reserves the right to monitor my work emails, phone calls, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

Name of staff	
Job title	
Department	
Signed	
Required Password	
Date signed	

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 IT Co-Ordinator.

Name		Department	
Equipment required			
First date of loan		Return date	

Pupil Acceptable use Agreements

School Network

Keep your password private, do not share this with others

Always log off when you have finished using the PC.

Email

You can send and receive personal e-mails. However, because we are a school emails will be monitored to see if they follow school rules.

1. Emails should not contain rude or inappropriate language.
2. When sending an email, you must be with a member of staff at all times.
3. You must only email addresses that staff say it is ok to use.

The internet

When you use the internet, staff will check to see if the website is ok for school use. This must be legal and not show aggression, use bad language or contain anything inappropriate.

None of the above material may be stored in your account.

Do not download anything without checking with staff first.

Your school account may be checked by the administrator at any time. Any areas of concern will be discussed with your Teacher and the Designated Safeguarding Lead.

You must not use any social networking site, e.g., Facebook, X, Instagram or TikTok while at Robert Ogden School

You are not allowed to use chat to speak to friends over the Internet not even while playing a game. This includes any game on ROBLOX.

Be careful what you share online, do not share personal information unless you check with your staff first.

Electronic devices

We do not permit pupils to bring in laptops, tablets, gaming devices, MP3 players or storage devices in school.

Mobile phones brought into school must be stored in reception or an agreement with your teacher to store away in an alternative place.

You must be supervised at all times.

If there is a problem, we will need to let other people who can help you know about this. Parents, Teachers will be told about the problem and decide what to do. This may mean you cannot use the computers, email or the internet.



Robert Ogden School



Email



You must be with staff when sending an email.



Only use email addresses that staff say are ok to use.



Internet



We only use the Internet when staff are with us.



Do not download anything without checking with staff.



We do not use social networking websites at school.



Tablet or Camera



Do not take photos or videos of staff or pupils unless staff say it is



ok.

Dear Parent/Carer

All pupils at the Robert Ogden School use computer facilities and internet access as an essential part of learning. Your child will have the opportunity to access a range of information and communication technology (ICT) resources. This may include access to:

- Chromebooks, including Google Suite and Google Classroom (a kind of learning platform)
- Other computers, laptops and digital devices
- The Internet, which may include search engines and educational sites
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

The school recognises the essential and important contribution that technology plays in promoting children's learning and development, and believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. To support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and discuss the content with them. Hopefully, you will also find this Acceptable Use Agreement provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home. We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home.

Full details of the school's online safety policy are available on the school website or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/online-safety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact