Online Acceptable Use Policy and Guidance

Introduction & Aims	

Our school strives to create a positive, safe and caring environment where children have a strong sense of belonging and staff work hard to build positive relationships with all pupils, parents and members of our school community. "Achievement by All" lies at the heart of what we do and we live our five core values of kindness, respect, imagining, resilience and reflection. Using technology is an integral part of the way our school works – it supports teaching and learning, and the pastoral and administrative functions of the school. Information Communications Technology (ICT) resources and facilities our school uses could also pose a risk to data protection, online safety and safeguarding.

This policy aims to:

- set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- establish clear expectations for the way all members of the school community engage with each other online
- support the school's policies on data protection, online safety and safeguarding
- prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. A list of definitions and glossary of terms can be found in the appendix.

It is our aim to recognise and celebrate the diversity of our school population and to also ensure that all children make progress so that 'Achievement by All'.

Legislation	

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011

- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

Unacceptable Use	

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.
Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities

- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard) inappropriately.
    - For children to write their homework or class assignments, where AI-generated text or imagery is presented as their own work
    - For staff to enter sensitive data such as personal data, for example entering pupils' names into a ChatGPT

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

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

Staff (including Governors, Volunteers, & Contractors)	

The school's Senior Admin Assistant with AgileICT, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.
Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Senior Admin Assistant.

School Email Addresses and School Mobile Phones

The school provides each member of staff and school governor with an email address which should be used for work purposes only. Anyone with a school email address should follow good practice, as follows:

- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted, if not being sent to another work email from Hampshire Children's Services.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the Headteacher and Data Protection Officer and school will follow our data breach procedure.

In additional to this, staff must not give their personal phone number(s) to parents/carers or pupils. If staff are issued with a school mobile phone they must use phone provided by the school to conduct all work-related business and chool phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in this policy.

Personal Use

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

- Does not take place during teaching time
- Does not constitute 'unacceptable use', as outlined in this policy
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.
Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.
Staff should take care to follow the school's guidelines on use of social media (Appendix Three) to protect themselves online and avoid compromising their professional integrity.

School WIFI

Anyone who has access the school wifi, has to sign our terms and conditions. They should also be made aware that if they are connecting from a personal device, that any browsers, apps running the background, etc. and that the school network monitoring will collect this data. It is advised that apps, open websites, etc. which are not appropriate are closed.

Personal Social Media Accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

Remote Access

We allow staff to access the school's ICT facilities and materials remotely – they should dial in using a virtual private network (VPN). The Headteacher oversees Remote Access and staff should contact the Headteacher to get access. Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

School Social Media Accounts

The school has some official accounts, managed by the Headteacher and also Senior School Staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

Monitoring and Filtering of the Schol Network and ICT Facilities

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

- internet sites visited
- bandwidth usage
- email accounts
- user activity/access logs
- any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation

- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Governor Role

Our governing body is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

Pupils	

Pupils have access to ICT facilities, such as laptops and ipads as part of their daily use. They are always under the supervision of staff.

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

- poses a risk to staff or pupils
- is identified in the school behaviour policy as a banned item for which a search can be carried out and
- is evidence in relation to an offence

This includes, but is not limited to:

- pornography
- abusive messages, images or videos
- indecent images of children
- evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Designated Safeguarding Lead.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- cause harm
- undermine the safe environment of the school or disrupt teaching
- commit an offence

If inappropriate material is found on the device, it is up to the Designated Safeguarding Lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

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

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

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

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

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

Unacceptable Use of ICT and the Internet Outside of School

The school will follow procedures outlined in the school behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- using ICT or the internet to breach intellectual property rights or copyright
- using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

- breaching the school's policies or procedures
- any illegal conduct, or making statements which are deemed to be advocating illegal activity
- accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- activity which defames or disparages the school, or risks bringing the school into disrepute
- sharing confidential information about the school, other pupils, or other members of the school community
- gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ict facilities
- causing intentional damage to the school's ict facilities or materials
- causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- using inappropriate or offensive language

Artificial Intelligence (AI)	

Generative AI means artificial intelligence tools that generate new, 'natural'-seeming content - i.e. it seems like it was created by a person, not a computer. Tools include:

- Chatbots such as ChatGPT, Google Bard and GrammarlyGO, which generate text
- Text-to-image programs such as DALL-E and Midjourney, which create images

Staff shouldn't enter sensitive data into a generative artificial intelligence (AI) tool if they are not sure how it will use or store the data. Many tools are available as personal or consumer products, so they may not meet the legal requirements for data handling.

Technology platforms and products (such as MIS and cloud storage) are increasingly using AI. However, many of these are designed to be used by companies and will comply with your data handling requirements.

You should avoid entering data into:

- consumer products that aren't designed for sharing institutional data
- tools which don't align with your data practice processes – for example, ones that allow your data to be used for AI training

Be especially cautious with:
Personal data: information from which someone can be directly identified, or identified when the information is combined with other information. For example:

- A name

- An identification number, such as an IT login
- Location data, such as your school name

There is guidance on personal data from the Information Commissioner's Office (ICO) for more information.

Special category data: personal data which could pose significant risks to an individual's rights and freedoms if it's lost or stolen. For example:

- Data revealing:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
- Information concerning:
  - Biometrics (such as fingerprints, or retina scans), where used for identification purposes
  - Health, including physical or mental
  - Sex life
  - Sexual orientation

Read more about special category data under the UK GDPR.

Photographs **are also data**, and may fall into personal and special category data categories.

The DfE highlights the need to protect personal and sensitive data in its guidance on handling generative AI in schools.

Treat AI Tools as you would any other system

Don't enter information into an AI tool if:

- You're not sure if it meets the legal requirements of a data processor
- You don't have the data subject's permission to do so

For more guidance, see our articles on the UK GDPR and seeking consent for processing personal data.

For example, staff should not use:

- ***Use ChatGPT to write anything that contains pupils' names***
- ***Enter sensitive data into an AI tool to help plan a safeguarding report***
- ***Use pictures of pupils as part of a prompt for image-generating AI tools***

If you're unsure, check your data protection policies and ask your data protection officer (DPO) what the risks are for a specific activity.

Pupils' Original Work, Consent and AI

Most AI tools use the information submitted by users to train and improve their outputs. However, intellectual property (IP) can only be used to train AI if the rights holder gives consent. Pupils own the IP rights to any original content they create. Original work is likely to include anything that shows working out or is more than multiple choice questions.
Staff **must not** allow or cause pupils' original work to be used to train generative AI unless you have appropriate consent. For pupils under the age of 18, staff will need the consent of their parents/carers.

Some AI tools allow users to opt out of inputs being used for training.
This is explained in the DfE's guidance on using AI in education (linked above).

Suspicious Emails

Generative AI tools can be used by cyber attackers to create convincing scam emails. Scammers may send fraudulent emails written by chatbots which:

- Contain malware in links or attachments
- Pretend to be from a specific person asking you to send sensitive data (known as 'spear phishing')
- Request a reasonable-sounding payment

For example, a scammer may pretend to be a parent/carer or a staff member emailing from a personal account. They could send a seemingly plausible request for you to send them information about 'their' child, or contact information for a teacher.
Look out for:

- Email addresses that don't match the contact details you have on file
- Generic email addresses, e.g. IT@trustname.com – check if these are actually used by your organisation
- An unusual tone – for example, an uncharacteristically formal message from a colleague or parent/carer
- Messages demanding urgent, time-sensitive action
- Suspicious links, containing strings of numbers or not matching where the link is claiming to take you – if you hover your mouse over the link, you can see the website it links to
- Generic introductions (e.g. 'Dear Sir or Madam')
- American spellings

Exercise the same vigilance and data protection practices you already have in place. These emails are no different to previous cyber attacks, but AI may allow scammers to be more convincing and carry out a greater number of attacks.

If staff have any doubt about an email, check the identity of the person who sent it before sending any information – for example, through a phone call.

Make sure to report any scam emails to your DPO and every effort will be made to inform the person who has had their identity compromised. Good practice means that school staff will report email scams to the police, as it maybe that this email could be used for illegal or activity which is not in line with the Standards for Headteachers.

AI Privacy Information with Pupils

As far as possible, we will teach pupils so they know what risks to look out for, and remind them that they should be careful with sensitive data when using AI tools. The risks of AI are shared, when staff would normally includes lessons about online privacy – for example, in PSHE or computing lessons.

Parents/Carers	

Parents/carers do not have access to the school's ICT facilities as a matter of course. However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion. Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the School Online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents and Carers play a vital role in helping model this behaviour for their children. Our school has a Parent Charter (Appendix Two) which makes reference to appropriate use of social media. This is also available on our school website.

Data Security	

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

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

- firewalls
- security features
- user authentication and multi-factor authentication
- anti-malware software

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. In some cases, passwords are allocaed initially by the Senior Admin Assistant/Senior Staff and staff are required to change them on first using them.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face further action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Pupils only have passwords for their online platforms and not for access to their school accounts on school devices.

Software Updates, Firewalls and Anti-Virus Software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

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

Any personal devices using the school's network must all be configured in this way.

Data Protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Access to Facilities and Materials

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

These access rights are managed by Senior Admin. Assitant and/or Headteacher. Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Senior Admin Assistant and Headteacher immediately.

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

Protection from Cyber Attacks	

Please see the glossary (appendix) to help understand cyber security terminology.

The school will:

- Work with governors and the AgileICT to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe at least annually, to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data on our school sytem happens overnight and store these backups on a cloud based system managed by Agile ICT.
- Our school uses other cloud-based procedures, such as CPOMs (for safeguarding) and Provision Maps (SEND software), Arbor (MIS system). These also have backups of data stored overnight.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Internet Access	

The school's wireless internet connection is secure. Pupils can only access this through school devices. Parents/carers and visitor are not permitted to use the school's WiFi unless specifically granted by the Headteacher.

The headteacher will only grant authorisation if:

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

Monitoring and Review	

The headteacher and safeguarding leads will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

This policy was agreed on…..

Appendix One: Terms Related to Online Acceptable Use

These terms include terms from the National Cyber Security Centre (NCSC).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Authorised Personnel	Employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Generative AI	Artificial intelligence tools that generate new, 'natural'-seeming content - i.e. it seems like it was created by a person, not a computer. Tools include: • Chatbots such as ChatGPT, Google Bard and GrammarlyGO, which generate text • Text-to-image programs such as DALL-E and Midjourney, which create images
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
ICT Facilities	All facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service.
Malware	Malicious software. This includes viruses, trojans or any code or content that can

TERM	DEFINITION
	adversely impact individuals or organisations.
Materials	Files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Personal Use	Any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Users	Anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix Two : Parental Charter

At Church Crookham Junior School we all want the best for every learner as 'Achievement by All' lies at the heart of all we do. Our school values are kindness, respect, imagination, resilience and reflection. The purpose of our charter is to capture how we all work together and communicate in the best interests of our children. The overarching expectation is that we have a mutual respect for each other and form a safe and productive environment to exchange information and provide a consistent message about the importance of learning and attending school.

This charter is based upon mutually agreeing the following themes:

Standards and Expectations

- *Support your child to ensure they come to school every day and being punctual and avoid taking any holidays during term time.* ***Evidence shows that children who achieve 95% attendance or higher make good progress.*** *This will give your child the best opportunity to achieve*
- *Support your child's participation in all aspects of school life and encourage them to join in a wide range of activities both during and after school*
- *Support and share the successes your child has outside of school so we can celebrate them together*
- *Support and encourage your child to follow our school values and expectations*
- *Support all school policies and procedures to ensure that the needs of all children can be best met*
- *Support the school's behaviour policy and help children to understand the three school rules of being safe, being kind and showing respect. We expect parents and carers to respond to any incidents in a structured and rational way, working alongside staff within our school*
- *Parents and carers support the three school rules in modelling these in your behaviour in and around the children at all times*

Communication between Home and School

- *Keep school staff informed of any changes of address or contact numbers*
- *Inform school before 9am of your child's absence and reason for absence*
- *Make sure the school is aware as early as possible of any circumstances that may affect your child's learning opportunities and wellbeing*
- *Engage with all forms of school communication (e.g. newsletters/Google Classrooms, etc.) in order to best support and reinforce your child's learning at home*
- *Ensure* ***your child reads regularly at home and completes other homework, such as weekly spellings, maths and learning times tables***
- *Make attendance at Parents' Evenings a priority to celebrate your child's success and to discuss their progress*
- *Attend a range of events in school to support your child*
- *Communicate any issues in an appropriate manner. We will always do the same. Any intimidatory behaviour, physical or verbal abuse towards our staff will not be tolerated*
- *Use appropriate channels to share concerns. In the event of a concern or grievance, respond proportionately and not through social media,* ***including Whatsapp****. We always seek to resolve issues together*

Our school is committed to working in close partnership with children, parents, staff and governors to ensure that our children learn in a safe and secure environment, so ensuring 'Achievement by All'.

Appendix Three: School's Guidelines on use of Social Media

Purpose:
These guidelines ensure that our school uses social media responsibly and safely to celebrate achievements, share updates, and engage with our community.

1. Parental Consent

- We will only use photographs of children whose parents/carers have provided written consent.
- Consent will be reviewed annually and recorded securely.

2. Privacy and Identification

- Children will **not be named** in photographs published on social media or the school website.
- We will avoid including personal details such as age, class, or location alongside images.

3. Image Quality and Inclusion

- Where possible, we will avoid blurring faces or asking children to step out of photographs.
- We aim to capture inclusive, positive images that reflect school life while respecting permissions.

4. Platforms Used

- The school may publish photographs and updates on:
    - **Instagram** (for school visits)
    - **School Facebook page**
    - **School newsletters**
    - **School website**

5. Appropriate Content

- Posts will reflect the school's values and be positive, respectful, and age-appropriate.
- No images or content will be shared that could embarrass or compromise a child's dignity.
- Social media will not be used to share personal information, messages, etc. and school will follow the usual school protocols (such as, if a child is unwell on a trip school will contact the parent directly and not use social media to make contact).

6. Timing and Context

- Photos will be shared after events, not in real-time, to protect children's safety.
- Location details will not be disclosed until after the event has concluded.

7. Staff Responsibility

- Only designated staff members will have access to and post on official school social media accounts.
- All posts will be approved by the Headteacher or delegated senior leader.

- **Staff will use school devices for photographing events and not their personal devices.**
    - Exceptions may apply during school trips where a separate risk assessment has been completed and approved.

8. Safeguarding

- No images will be shared that show children in swimwear or other potentially sensitive contexts.
- We will follow safeguarding guidelines for online content at all times.

9. Copyright and Ownership

- The school will ensure that any images or media used are owned by the school or have appropriate permissions.