Northern Lights Learning Trust

Hart Primary School Primary School

Acceptable Use Policy

'To give all the opportunity to be the best that they can be and have fullness of life.'

Prepared by: Jade Tillson (Assistant Headteacher and Computing Lead)

Approved:

Signature Chair Local Governing Body:

Date of Renewal: Autumn 2027

Pastoral Care/Spiritual Development

The quality of relationships between all members of school staff and pupils, and the relationship with parents and carers is the area that is most commonly associated with the ethos of the schools in our Trust. It is expressed in the terms of sharing and caring. In the Church schools in our Trust, we follow the teachings of:

'Love your neighbour as yourself' – Matthew 22:39.

'This is my commandment: love each other' - John 15:17.

In our schools we believe every pupil is an individual who is valued for who they are.

We have a series of overlapping networks of relationships, which includes governors, staff, children, parents, church members, and members of the community which the school seeks to serve. Our pastoral work will strive to meet the significant challenge to create and maintain such networks including in our Church schools in ways which reflect the Gospel. Those who are in leadership roles, which includes all who have a particular responsibility, ensure that by their personal example they set the highest standards expected.

It is from this premise that both Christian and spiritual love will pervade all aspects of life at Northern Lights Learning Trust. It will influence how we reward and teach discipline. It will affect how we value work and the achievements of pupils and staff. It will be seen in the way in which the school environments are created and cared for, in the way in which the needs of pupils, parents, and community are met, and in the way in which teaching and non-teaching staff work together effectively as a team. Pastoral care pervades all aspects of school life and therefore will be reflected in the way the schools are organised and the policies are written and implemented.

Contents:

Statement of intent

1. Introduction
2. General policy and code of practice
3. Internet policy and code of practice
4. Email and Teams policy and code of practice
5. Email policy – advice to staff
6. Use of Mobile Technology
7. Use of AI (artificial intelligence)
8. Social Media Policy
9. Remote Learning
10. Further guidelines
11. Sanctions
12. Appendices – Acceptable Use Agreements

Statement of intent

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

This acceptable use policy is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Its main aims are:
• Set clear guidelines and rules for the use of school ICT facilities by staff, pupils, parents, volunteers, contractors and visitors.
• Establish shared expectations for how we communicate and engage online.
• Prevent disruption to learning and school operations through misuse of ICT systems.
• Support compliance with safeguarding, online safety and data protection requirements.

1. Introduction

This policy applies to all employees, pupils, parents, volunteers, supply staff and contractors using school ICT facilities.

1.1 The school acceptable use policy is divided into the following sections:

- General policy and code of practice
- Internet policy and code of practice
- Email policy and code of practice
- Remote learning

1.2 This policy MUST be read in conjunction with the school's Data Protection Policy, Privacy Notice and Records Retention Policy.

1.3 <u>Relevant legislation and guidance</u>
This policy aligns with:
• UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
• Computer Misuse Act 1990; Human Rights Act 1998
• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
• Education Act 2011; The Education and Inspections Act 2006
• Freedom of Information Act 2000
• Keeping Children Safe in Education (latest version) and DfE guidance on Searching, Screening and Confiscation
• National Cyber Security Centre advice and the DfE's "Meeting digital and technology standards in schools and colleges"

2. General policy and code of practice

Privacy

2.1 The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.
The school will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.

In order to protect pupils' safety and wellbeing, and to protect the school from any third-party claims or legal action against it, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The trust's Privacy Notice details the lawful basis under which the school is lawfully allowed to do so.

Code of practice

Staff will follow the school's values 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.

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.

Passwords should be strong and unique. Staff should use passphrases wherever possible and must not reuse passwords across systems. Multi-factor authentication (MFA) must be enabled where available.

Staff must not reuse passwords across different accounts.

Pupil devices may use age-appropriate sign-in. Staff must ensure that pupil passwords must not be written on devices or stored in plain text.

If you forget or accidentally disclose your password to anyone else, you must change your password and report it to the business Manager.

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 BusinessManager can monitor your use of the system. Use of the school's facilities by a third party using your username 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

When you are not working at your computer an automatic lock screen will appear and an online safety screensaver will appear. This screensaver (the SMART acronym) should not be removed or adapted. 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 and to the computer

You must not connect any hardware which may be detrimental to the school's network.

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 the computing and technology lead or SLT.

You may use portable storage media (such as school cameras and iPads) where a port is provided on the device. You are not permitted to connect anything else to the computer without first getting the permission from the computing and technology lead or a member of the SLT.

Virus

If you suspect that your computer has a virus, report it immediately via the approved IT support system and notify the Computing Lead.

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 and transferring files

You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require.

You may transfer files to and from your network using Teams to store and transfer files. The use of portable USB devises is not permitted on school devices unless otherwise stated by the Business Manager or SLT. Only approved school devices may be used to transfer personal data, and only with prior authorisation from the Headteacher/Business Manager

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. Staff must not use personal email or personal cloud storage for schoolwork.

Data breach and error handling

If personal data is sent in error (e.g., wrong recipient) or accessed/lost improperly, inform the Headteacher andBusiness Manager immediately and record the incident in the school's data breach log (via GDPRSentry). Do not forward, copy or further disclose the data.

Reporting faults and malfunctions

It is your responsibility to report any faults or malfunctions to the network manager IT Assist to log any issues - this must include full details and all error messages. You must also inform the computing and technology lead via email as soon as possible.

Food and drink

You must not eat or drink while using computer devices. 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 back-up copies, e.g. on the cloud or in a Teams folder, of your work, and you must keep copies of any important work that you might have. 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.

Devices

A centrally managed inventory of school devices is maintained by designated staff and reviewed termly by the Computing Lead and Headteacher.

Any changes in location of devices should be reported to the computing lead.

CPOMS

Any sensitive communication regarding a child should be done using CPOMS. CPOMS ensures that the appropriate adult is notified and a record is stored securely for each child.

3 Internet policy and code of practice

3.1 The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.
3.2 Whenever accessing the internet using the school's or personal equipment you must observe the code of practice below.
3.3 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.
3.4 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.
3.5 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?

3.6 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, filtering and monitoring services, licenses, technical support, 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.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and 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 normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that:

- Such use is occasional and reasonable;
- Such use does not interfere in any way with your duties; and
- You always follow the code of practice.

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 computing lead or SLT 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.

Filtering, monitoring and Wi-Fi access

Internet access on school networks (including domain-controlled and Wi-Fi connected devices) is filtered via Securly. User activity is monitored in line with safeguarding requirements. The system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.

Examples of unacceptable use include:
• Using ICT to bully or harass others; promoting unlawful discrimination
• Accessing, creating, storing or sending pornographic, extremist, racist, antisemitic or otherwise harmful content
• Sharing nude or semi-nude images (consensual or non-consensual), including via livestreams
• Setting up software/web services without approval; using tools to bypass filtering
• Connecting unauthorised devices (including non-encrypted memory sticks) to the network
• Promoting a private business unless directly related to the school
(This list is not exhaustive; professional judgement will be applied.)

Guest access is time-limited and logged for specific approved purposes (e.g., on-site training).
If unsuitable content is accessible, report the URL and details to the Headteacher/ICT support so filtering can be updated.

Giving out information

You must not give any information concerning the school, its pupils 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. Signing up to any subscriptions should be discussed with the computing and technology lead or SLT prior to purchase even if the subscription is free.

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.

4 Email and Teams policy and code of practice

4.1 The school's computer system enables members of the school to communicate by email and through Teams with any individual or organisation with email facilities throughout the world.

For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

Any breach of this policy and code of practice will be treated 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.

Code of practice Purpose

You should only use the school's email and Teams system for work related communication.

You are only permitted to send a reasonable number of emails.

Trust's disclaimer

The school's email disclaimer is automatically attached to all external outgoing emails and you must not cancel or disapply it.

Monitoring

Copies of all incoming and outgoing emails, together with details of their duration and destinations can be accessed by SLT.

The frequency and content of incoming and outgoing external emails may be checked to determine whether the email system is being used in accordance with this policy and code of practice.

The headteacher, senior staff and technical staff are entitled to have read-only access to your emails.

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 program 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 computing and technology lead or a member of SLT.

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 may 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, libellous, 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, libellous, 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.

You must not open or download attachments from unknown or unexpected sources.

If you receive any inappropriate emails or attachments you must report them to technical staff immediately.

Viruses

If you suspect that an email has a virus attached to it, you must inform computing and technology lead or SLT 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. For further information please see our Records Retention Policy.

Message size

Staff are limited to sending messages with attachments. If you wish to distribute files within the school, you can do so by using shared areas such as teams.

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.

Microsoft Teams
Microsoft teams should only be used to communicate with parents/carers when directed by SLT. This may be to meet with parents/ carers for consultations or during isolation periods. SLT will communicate to parents/carers and staff when this is appropriate.

Secure handling of email
• Use your school email for work purposes only; enable MFA when accessing off-site.
• Encrypt attachments that contain personal or confidential information. If using password protection, share the password verbally or in person – never by email.
• If you receive an email in error, inform the sender and delete it. If you send personal data in error, inform the Headteacher and Office Manager immediately and record the incident (see Data breach and error handling).
• Staff must use school-approved systems for parent communication.

5. Email policy – advice to staff

5.1 Staff should remind themselves of the Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them. There is no expectation that staff read or respond to emails out of hours.
- 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.
- Parents/carers must email admin or info account and not staff directly. Staff must not communicate with parents via their personal/school email.
- Where appropriate, use scheduled send features to avoid out-of-hours alerts for recipients.

Data security and cyber protection
We aim to meet DfE digital and technology standards and follow NCSC guidance. Key controls include:
• Firewalls, anti-malware, endpoint detection/response, regular security patching
• Multi-factor authentication and secure password management for staff
• Nightly on-site and off-site backups of critical files and weekly server OS backups; periodic restore tests
• Regular access reviews to ensure users have the correct permissions and admin rights
• Supplier assurance for critical services (e.g., Cyber Essentials)
• A documented incident response plan (including how we will communicate if systems are unavailable) which

we test and review after significant events
Staff receive regular cyber-security training (including phishing awareness and payment change verification) and must report suspected incidents immediately.

6. Use of Mobile Technology

We recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Use of phones by staff

6.1 Staff are not to use mobile phones during teaching time or in any learning environment. This ensures that there is a reduced risk of any digital images. This includes making and receiving calls, sending/receiving text messages and accessing the Internet from a mobile phone. Mobile phones must be locked in staff lockers and may be accessed in offices, staffrooms and in the staff cloakrooms [ie where children have no access] during staff breaks. The door to the office corridor from the staff area, must be closed if any member of staff is using a mobile phone.

Whenever possible, staff should use a land line to make calls for work related purposes.
If staff are out on trips or courses, in emergencies [accidents, bus delays, children ill etc] staff may use their personal mobiles to contact the school or emergency services.

Use of phones by pupils

6.2 There is no reason for children to bring mobile phones to school. We appreciate, however, that there are occasions when it is useful for parents to be able to contact older children directly by mobile telephone: this applies particularly to those pupils who travel to or from school alone.

Generally, children should not bring a mobile telephone to school. The school office will assist if they need to make a telephone call home; and the School Administrator is always more than willing to allow children to ring home from the office when that is appropriate.

If a mobile telephone is brought to school by a child, [for emergency travel purposes] the school can accept no responsibility for loss or damage to the telephone. As with all valuable property, the pupil should hand the telephone into the school office for safe keeping.
If a mobile telephone is brought to school, it must be switched off during the school day.
If a member of Staff discovers a mobile telephone in use by a child during the day, it will be removed, sent to the school office and may only be recovered by parents in such an eventuality.

Use of phones by parents

6.3 Parents/visitors are advised to switch off mobile phones in the vicinity of school. Volunteer helpers MUST switch off mobile phones whilst in the school.

No parent/visitor may use a mobile phone to take photographs of children to safeguard the welfare of all children and avoid data protection issues with regard to inappropriate capture, use or distribution of images.

Use of smart watches

6.4 Smart watches capable of recording audio, capturing images or connecting to the internet must not be used during lessons or when supervising pupils; disable notifications where they may distract from professional duties.

7. Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

The school recognises that AI-generated content, including images, videos, audio and text, may not always be accurate or genuine. Pupils will be supported to think critically about online content and to seek help from a trusted adult if they are unsure about something they have seen online.

The school recognises that AI can be used to create manipulated, synthetic or "deepfake" content. Such content may be misleading, harmful or constitute a safeguarding concern. Any concerns involving deepfakes or manipulated media must be reported in line with safeguarding procedures.

To ensure the safe, secure and appropriate use of artificial intelligence (AI), Microsoft Copilot is the only AI tool authorised for use within school.

7.1 - Policies:

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

7.2a - Safe use, data protection and security:

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into any AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only AI tools approved through the school's procurement, safeguarding and data protection processes may be used for school business. New AI tools must be reviewed before use.
- Safeguard sensitive information**.** Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

7.2b - Pupil responsibilities

Pupils must:

- Use AI tools only when authorised by a member of staff.
- Not submit AI-generated work as their own where this is prohibited by teachers or assessment rules.

7.3 - Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

7.4 - Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, safeguarding incidents, inappropriate outputs, suspected data breaches or misuse through the school's established safeguarding, data protection or incident reporting procedures.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular reviews.
- Engage parents/carers with clear information if AI is used in school.

7.5 - Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

7.6 - Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

The following uses of AI are prohibited unless specifically authorised by the Headteacher or designated lead:

- Entering personal, confidential or safeguarding information into non-approved AI systems.
- Creating content that is illegal, harmful, discriminatory, abusive or inappropriate.

8- Social Media Policy

8.1 Parents, carers, staff, governors, visitors and pupils must all refrain from discussing the Academy, uploading photographs of/or related to the Academy on social media websites (including Facebook, Twitter etc.).

Social Media for Staff

When using social media outside of school, staff must follow the following guidelines:

Change your display name so that you are not easily found online.

Ensure profile pictures are professional or change them to something that is unidentifiable.

Regularly check your privacy settings.

Be careful about tagging other staff members in images or posts.

- Don't share anything publicly that you wouldn't be just as happy showing your pupils.
- Don't make comments about your job, your colleagues, your school or your pupils online.

- Don't associate yourself with your school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
- Don't link your work email address to your social media accounts.

If a pupil adds you on social media, following the following steps:

- Ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils.
- Notify your senior leadership team or headteacher about what is happening.

It is not recommended that staff members accept friend requests from parents or carers.

Official school social media accounts

8.2 Where the school operates official social media accounts for communication with the community, access is restricted to authorised staff, and content must follow school guidelines. Personal social media must not be accessed via school ICT. See Appendix 1 for staff privacy guidance (Facebook).

9. Remote Learning

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions, as the headteacher may require from time to time, against importing viruses or compromising system security.

a. The school's computer system enables members of the school to communicate and teach remotely through the use of Teams with any individual within the trust and with agreed outside agencies.
b. For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of Teams by all. (See Appendix 1)
c. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.
d. 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.

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of the school when taking part in remote learning following any full or partial school/setting closures.

Remote learning will take place through recorded sessions and live sessions using Teams. Teams has been assessed and approved by the headteacher and trust. Live streamed remote learning sessions will only be held with agreement from the headteacher/a member of SLT.

Staff will only use the school managed or specific, approved professional accounts with learners and/or parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

Any pre-existing relationships or situations which mean this cannot be applied will be discussed with SLT.

Staff will use work provided equipment e.g. a school/setting laptop, tablet, or other mobile device.

Loaning devices to pupils/staff

Devices are available for loan and if you require a device to complete remote learning this should be discussed with the computing lead or SLT. A contract should be signed by any individual loaning a device (Appendix 2) and a record of when the device was loaned/brought back to school will be kept.

Pupils may also loan devices and parents will be asked to sign a contract which details acceptable and unacceptable use of the device (Appendix 2). A record of when the device was loaned/brought back to school will be kept.

Remote access for staff

Staff should primarily use Microsoft Teams for remote collaboration and document sharing, following Trust guidance. Only school-managed devices may be used to access school data or systems when off-site.

Wifi code/Data cards

To ensure that all pupils are able to access remote learning wifi codes and data cards will be accessible. These will be accessible from the office staff or SLT.

10. 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.
- To support staff work life balance and differing personal circumstances, emails can be sent at any time but it is accepted that they are not read/responded to outside of the typical working day.
- 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.

11. Sanctions

Breaches of this policy may be addressed under the school’s/Trust’s Code of Conduct and Disciplinary Policy for staff, and Behaviour; Suspension and Exclusion policies for pupils. The Headteacher will apply professional judgement to determine appropriate action, including where unacceptable ICT use occurs off-site but impacts the school.

For further information or to clarify any of the points raised in this policy please speak to the DPO via the schools DPL or the trust senior DPL.

12.– Appendix 1: acceptable use agreement (pupils, parents/carers).

RESPONSIBLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
In school, 1. I will ask permission before using the Internet; 2. I will use only my own network login and password; 3. I will only look at or delete my own files; 4. I understand that I must not bring devices into school without permission 5. I understand that if I do bring in a device, my teacher will be informed, and it will be locked away by the office staff until home time; 6. I will only e-mail people I know, or my teacher has approved; 7. The messages I send will be polite and sensible; 8. I understand that I must never share personal information online, including my home address, phone number, photographs, passwords or location, or arrange to meet someone I have only met online. 9. I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know; 10. I will not use Internet chat; 11. I will only access online games and activities approved by my teacher. 12. If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately; 13. I understand that the school may check my computer files and the Internet sites I visit; 14. I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers, and my parents will be informed. 15. I understand that some online content may be created using artificial intelligence (AI). If I am unsure whether information, images or videos are real or trustworthy, I will ask a teacher or trusted adult.	
<u>Pupil Agreement</u> I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed (pupil):	**Date:**
<u>Parental Consent for Internet Access</u> I have read and understood the school Rules for Responsible Internet Use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school uses filtering and monitoring systems to help keep pupils safe when using technology. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I agree to this for the duration of my child's time at Hart Primary School.	
Signed (parent/carer):	**Date:**
Please print name:	

Appendix 2: acceptable use agreement (staff, governors, volunteers, and visitors).

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Use social networking sites or online communication platforms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take, store or share photographs, video or audio recordings of pupils except in accordance with school policy and authorised school procedures. • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will report any suspected data breach, cyber security incident, phishing email or loss of school equipment immediately in line with school procedures. I will inform the Designated Safeguarding Lead (DSL) if a pupil tells me they have found material online that could upset, distress or harm them or others, or if I encounter such material myself. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too. I will only use AI tools that have been approved by the school and will not enter confidential, personal or sensitive information into AI systems unless explicitly authorised by the school. I understand that content generated by AI must be checked for accuracy, bias, copyright and safeguarding concerns before use. I understand that the school's systems are subject to filtering, monitoring and security controls to support safeguarding and cyber security.	
Signed (staff member/governor/volunteer/visitor):	**Date:**