Northern Lights Learning Trust

Hart Primary School

Acceptable Use Policy

Prepared by: Jade Tilson (Computing Lead)
Approved: Katy Hill
Signature Chair Local Governing Body:
Date of Renewal: Autumn 2024

Contents:

Statement of intent

1. Introduction
2. General policy and code of practice
3. Internet policy and code of practice
4. Email policy and code of practice
5. Email policy – advice to staff
6. Remote Learning
7. Further guidelines

Northern Lights Learning Trust

Signed off by: Chair of MAT Board
Date from: Spring 2022
Review Date: Autumn 2024
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.

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.

1. Introduction

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

1.2. 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

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

2. General policy and code of practice

2.1. The school's ICT systems are in place for you to benefit from.

2.2. This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

Privacy

2.3. 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.

2.4. 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.

2.5. 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.

Your password must be a mix of the following:

- Contain at least six characters
- A mixture of lower case and capital letters
- At least one numbers
- At least one symbol

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

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

Connections to the computer

You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of 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, you must report it to the computing coordinator and log it onto the portal for the Office Manager to look into.

Installation of software, files or media

You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers.

You must not alter or re-configure software on any part of the school's system.

File space

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

Transferring files

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 Office Manager or SLT.

When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.

Reporting faults and malfunctions

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 log of devices is kept and managed by the computing and technology lead. This inventory is checked on a termly basis by the digital leaders in school and overseen by the computing and technology lead.

Any changes in location of devices should be reported to the computing and technology 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, 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 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.

Monitoring

The internet access 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.

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.

4.2. 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.

4.3. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

4.4. 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 maybe have to be disclosed as part of fulfilling an SAR
- Whether any authorisation is required before sending
- Printed copies of emails should be retained in the same way as other correspondence, e.g. letter
- The confidentiality between sender and recipient
- Transmitting the work of other people, without their permission, may infringe copyright laws.
- The sending and storing messages or attachments containing statements which could be construed as abusive, 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.

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.

6. 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.

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.

6. 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.

6.1. 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.

6.2. 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)

6.3. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

6.4. 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.

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.

Appendix 1

School Laptop Declaration

Please read and sign for the loan and use of a school's laptop and equipment. A record of this declaration will be kept in school. Please be aware that laptops will be subject to random checks by senior management and NLLT. Laptops are owned by the school and are to be used by staff to enhance their professional activities including teaching, research, administration and management.

This declaration is to be read in conjunction with the school's "Acceptable Use Policy".

It is required that all school laptops:

• be used primarily for school business and private use shall be ancillary and not significant otherwise tax liabilities may be incurred.

• Should be used for activities appropriate to staff professional needs.

• May be used for personal use at the discretion of the head teacher without damaging the integrity of the school, and school systems.

• Must never be used for accessing or purchasing inappropriate materials such as pornographic, racist or offensive material, or for personal financial gain, gambling, political purposes, advertising, or accessing chat rooms.

• Should only be used by the named person signing this declaration or under strict supervision of this person. The person signing this declaration is solely responsible for any material accessed via the laptop, and to this end, may face disciplinary action should inappropriate use occur.

• Should only be accessible via a password, known only to the user and senior management of the school.

I also declare the following:

• I will use the schools e-mail, internet and intranet facilities primarily for business use, and only for personal use during designated break/holiday/home periods in line with ICT use policy.

• I will use only those facilities I am authorised to use.

• I understand that my usage of these facilities may be monitored in accordance with our Data Protection Policy/ICT Use Policy

• I understand this declaration applies to all other mediums and equipment. I am aware and understand the above requirements of the school and local authority, have read guidance, and will adhere to these guidelines.

Name (in print) _____

Signed _____ Date _____

Appendix 2

Chrome Book Sign Out

Name	Chromebook	Date out	Staff Name	Staff Signature	Date in	Staff Name	Staff Signature