Acceptable Use Policy

Adults

Including Data Protection/GDPR Quick Checklist

September 2021

Approved by:	[Name]	**Date:**	[Date]
Last reviewed on:	[Date]		
Next review due by:	[Date]		

Aims and objectives

The purpose of the policy is to ensure the school network is operated safely and all users of ICT are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

This document outlines the key points of our AUP. It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under and how to work safely particularly in the areas of data protection and safeguarding.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face disciplinary action and in the most serious cases legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible **it is your responsibility to make sure the pupils you are directly working with are safe**. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

Key responsibilities

Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect pupils.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the head teacher
- Supporting pupils who experience problems when using the internet.
- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using child-oriented search engines.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
- Gaining permission to use any new methods of collecting or storing personal or sensitive information- eg new apps which require input of pupils' personal data.
- Copies of our rules for pupil use of the network are displayed around the school. Please ensure you have read them and make sure the pupils you work with adhere to them.
- Ensuring that personal data is stored securely and is used appropriately, whether in the building, taken off site or accessed remotely. Encrypted memory sticks will be used when any pupil information (reports, assessment data etc) is taken off site. No personal data or photographs should be stored on any unencrypted memory sticks or disks.
- Staff mobile phones should not be used during lessons or when children are present. They should be switched to 'silent' mode or turned off when on site and should be left either in the staffroom or left in the School Office so that they are not accessible by children. When possible, all mobiles should be locked with a PIN/password.
- Images of students must be stored in the designated area of the IT network (hard drive) and kept in a time frame identified in the Digital Images Policy. It is not permitted to remove images off site (on camera, phone or storage device).

School ICT Network

The school Network and associated services may be used for lawful purposes only.

Passwords

- Each adult working within the school must log on to the computers using the username and password given to them (class account or individual account) and these must be changed to an individual specific password where stated. Passwords need to be kept a secret, not written down and stored in or around the computer. If for any reason a person needs to leave their computer unattended, they must lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.
- Any supply teachers or visitors to the school must see our head teacher to obtain a guest account and password. Their password will need to be kept private and not shared.
- You should ensure you use dual factor authentication when possible if dealing with sensitive information- for example CPOMS.

Software and Downloads

- All users of the network must virus check any device storage devices before using on the network. All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the head teacher. If users need a new program installing onto the computer, our ICT Technician will be asked to do this if possible.
- Copyright and intellectual property rights must be respected when downloading from the internet.
- Any memory USB stick used must be encrypted and should only be used if they are provided by the school.

Personal Use

The school recognises that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Must comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Offsite activities

If you have a need to work offsite and require electronic or paper-based information to be taken from school to work on you must:

- First seek permission from the head teacher for the removal of the information eg pupil file, laptop, encrypted memory stick
- Ensure the secure transit of the information
- Ensure that no information is downloaded or stored on personal equipment
- Be aware of other people within the immediate area when viewing personal or sensitive information in areas outside of school and limiting such activity away from public places

Pupil data should always be stored on the One Drive either in a personal or whole staff area as appropriate. You should not therefore transport paper-based or electronically-saved information from school to home. If you have a need to remove any personal or sensitive information from the school, then you should seek permission from the Head Teacher.

Email

- All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.
- No member of staff must use non-school email accounts for any school/work related activity.
- Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public.
- Email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
- E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or any other minorities. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- All emails both sent and received will be scanned by forensic software.
- E-mail attachments should only be opened if the source is known and trusted.
- Privacy – you will not reveal any personal information (e.g. name, address, age, telephone number, social network details) of other users to any unauthorised person. You will not reveal any of your personal information to pupils.
- You will not trespass into other users' files or folders.
- You will ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than yourself. Likewise, you will not share those of other users. Ensure that if you think someone has learned your password then you will change it immediately and/or contact the head teacher.
- If you are required to email personal or sensitive information, ensure that the email is encrypted, and that the information is being sent securely.
- If you are required to send an email to more than one recipient, ensure that the email addresses are entered in to the 'bcc' box to ensure that you are not sharing personal email addresses with others.
- Ensure that you log off after your session has finished. If you find an unattended machine logged on under another username do not continue using the machine – log it off immediately.
- Any unsuitable communications received must be reported to a member of staff immediately.
- If required to email sensitive information you will use a double-checking system whereby you ask another appropriate member of staff to check the content before sending.

Images/Videos

- All pupils need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect others' files and content. Do not corrupt, interfere with or destroy them.
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

Photocopiers/Printers and Scanners

- If printing or scanning documents, ensure that any document containing personal or sensitive information is only printed at a time when you are able to collect it immediately, so as not to leave sensitive information lying on printers/photocopiers

Internet Usage

- Pupils must be supervised at all times when using the internet.
- Activities should be planned so 'open searching is kept to a minimum.
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines.
- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is only allowed during break and lunchtimes or after school and only in areas where no children are present.
- Do not use the internet for personal financial gain, gambling, political purposes or advertising.
- Do not attempt to visit websites that may be considered inappropriate or illegal. Be aware that downloading some material is illegal and that the police or other authorities may be called to investigate.
- Do not try to upload, download or access any materials which are illegal (Child abuse images, criminally racist material, adult pornography covered by the obscene publications act) or inappropriate or may cause harm or distress to others. I will not try to use programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time on their own computer at home. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your 'friends list', nor invite them to be friends with you.
- You must ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- You should avoid contacting any pupil privately via social networking site, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.
- You should not name the school as your place of work on social networking sites.
- You will not discuss the school, its staff, its pupils, its families or agencies involved in the life of the school on social networking sites.
- You will not make inferences about my daily routine on social networking sites when it could be interpreted negatively or breach confidentiality.

It is advised not to accept invitations from the pupils' parents or carers to add you as a friend to their social networking sites, nor should you invite them to be your friends, as damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- No school related information should be stored on any personal equipment.
- You must not connect personal computer equipment to school computer equipment without prior approval from the head teacher.

Mobile Devices

- Personal mobile phones should not be used in areas of school where pupils have access.
- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard or locker away from the children.
- Adults are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room (safe, suitable places where the children are not present).
- It is forbidden to take photographs/videos of the children on personal mobile phones.
- No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from the head teacher.

Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Reporting Problems with the Computer System

It is the job of the ICT Technician to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- You should report any problems that need attention to the Head teacher/ICT Technician.
- If you suspect your computer has been affected by a virus or other malware, you must report this to the Head teacher/ICT Technician immediately.
- If you have lost documents or files, you should report this as soon as possible to the Head teacher or Data Protection Officer. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the Head teacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

All reports will be treated confidentially.

Reporting Data Breaches

Any data breach involving personal or sensitive information, such as loss of paperwork, memory stick, laptop or sending sensitive information to the wrong recipient, for example, should be reported immediately to the schools Data Protection Officer – Darren Hobson.

Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

Data Protection statement

I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

I have read, understood and agree to comply with the AUP:

Signed: ____ Date: _________

Print Name: _____________________________________

Position in School: ________________________________

Thornley Primary School

Data Protection/GDPR Quicklist

In order to comply with the Data Protection Legislation, we need to ensure the following actions are in place across school. Please note that 'data' refers to anything which could identify an individual e.g. name, image, DOB, address.

The guidance is intended to compliment the Acceptable Use Policy which all staff are required to sign.

- Laptops need to be encrypted. Until all laptops are updated please ensure that no personal data is stored on the laptop. If you are unsure if your laptop is encrypted, please speak to the ICT Technician
- All memory sticks must be encrypted and supplied by school
- Personal equipment should not be used for school purposes eg laptops, memory sticks, mobile phones or other devices
- School laptops should not be used by friends or family members
- Personal email accounts should not be used for work purposes
- All paper-based information should be shredded when no longer required
- When emailing data, the email/information must be encrypted. This can be set within emails on office 365. If you have any issues, please speak to the ICT Technician
- Information about pupil SEN as well as safeguarding and child protection information is considered sensitive data and must be kept in locked filing cabinets at all times and never taken home
- Ipads cannot be encrypted and should not be used to store sensitive data
- Pupils should never be allowed to use a computer accessed by a teachers' login
- All computers MUST be locked whenever they are left unattended using ctrl+alt+del
- Data sources (paper and electronic) e.g. laptops, assessment files must be kept secure at all times if they are taken out of school – permission must be sought before taking any data out of school.
- All data sources e.g. assessment information, pupil assessment folders, markbooks, IEPs must be kept secure – in locked filing cabinets/cupboards. We must have a 'tidy desk' approach every night and ensure that everything is locked away prior to leaving school.
- Letters containing pupil information e.g. referrals, must be hand delivered or sent securely and the contents double checked before sending
- Data sources will not be kept unnecessarily e.g. markbooks will be shredded once no longer used.
- Memory sticks should be used to transport information only and the data should be deleted once transportation is complete
- Passwords must;
    1. Be at least 8 characters – a mixture of numbers and letters. It is possible to make this something memorable by substituting letters/symbols for characters e.g. T40Rn13Y
    2. NEVER be given to anyone else e.g. supply teachers, apprentices
    3. Use a different password for different log ins in school – maybe just add an extension to avoid having to write anything down

Signed………………………………………………………………………

Date…………………………………………………………………………