Manby Lodge Infant
School (Staff) Acceptable Use of Technology Policy

Reviewed: Autumn 2023
Next review due: Autumn 2024

Technology has developed over recent years and is continuing to evolve. Particularly, during the Pandemic, we saw children using the internet more than they had ever done before.

The internet contains a wealth of information as well as having a profound effect on the way we communicate including instant messaging, emailing and text messaging.

Educational practitioners and their managers should be expected to use a range of technological resources to manage their roles as professionals; to be enabled to use the internet to research and communicate professionally; to use online systems to track and record the progress of children and young people and to share their work; to communicate with parents and carers through newsletters, email or the internet and to be able to manage administrative tasks and systems. All of these should be referenced as areas that require clear agreements regarding acceptable use; and must be recognised for their direct and indirect value in supporting the learning and development of children and young people.

In order to be effective, policies and procedures must be rigorous, enforced, monitored and reviewed to ensure they are to remain fit for purpose. Furthermore, it should be considered essential that all staff have a clear understanding of what will be considered acceptable and unacceptable behaviours. This should help to ensure the behaviour of ICT users will not be open to misinterpretation or lead to allegations as a result of any individual's lack of knowledge of the potential risks.

Mobile Phones
Mobile phones and personally-owned devices may not be used during the school day, except in the case of an emergency. They should be switched off or on silent and left in a safe place. They should be out of sight during lessons, assemblies and whilst moving throughout the school.

It is not appropriate at any time to take/store photos or videos of children during the school day on your own personal device. Staff are not permitted to use their own mobile phone to send pictures/videos to pupils or parents at any time, unless in an emergency. Staff should never send, or accept from anyone, texts or images that could be viewed

as inappropriate. If a member of staff suspects a message, text or similar may contain inappropriate content then the DSL should be informed.

Possession of Images
There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven. Adults should not use equipment belonging to their school/service to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. Adults should ensure that children are not exposed to any inappropriate images or web links. Settings and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Any abusive, inappropriate or illegal misuse of ICT equipment by a practitioner or manager should be reported immediately to the registered person. Where misuse relates to abuse and safeguarding, Children's Social Care, the Local Authority Designated Officer, Ofsted or the Police must be notified as applicable.
In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for educational practitioners or their managers to engage in personal online communications with children and young people, parents or carers.

E-mails
Staff must be aware that all incoming and outgoing emails can be read by our web host manager. This is not intended to infringe on staff privacy, but the internet is a very public way of communicating and like all companies, management reserves the right to ensure that the name of the school is not brought into disrepute.

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if a school computer was being used to look at inappropriate web pages.

Social Networking
Due to the increasing personal use of social networking sites, staff and volunteers within the workforce should be aware of the impact of their personal use upon their professional position.

In practice, anything posted on the Internet will be there forever and is no longer in your control.

Remember when something is on the Internet even if you remove it, it may have already been duplicated by a "web crawler" and so will always be there. Current and future employers and service users may see this. Keep all professional work completely separate from your private life.

The following guidance, in addition to the above, will safeguard adults from allegations and protect an individual's privacy as well as safeguard vulnerable groups.
Failure to comply with the following may result in organisations taking disciplinary action.

Staff must be aware of their responsibilities to Manby Lodge when using social networking sites such as Facebook. Our confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional.

- Staff should not foster online friendships with parents.
- Staff should not be part of whats app groups that include parents from school.

Disciplinary action could result if Manby Lodge is brought into disrepute.

- Staff must not post anything onto social networking sites such as 'Facebook' that could be construed to have any impact on Manby Lodge's reputation.

- Staff must not post photos related to the setting on any internet site including children, colleagues or parents.

- Staff must not post anything onto social networking sites that would offend any other member of staff or parent of Manby Lodge.

- Children are to be encouraged to use the internet if appropriate but must be supervised at all times.

All staff and volunteers at Manby Lodge will be given 'Safeguard Yourself' guidelines to read and sign off.

'Safeguard Yourself' Guidelines

Social networking sites such as Facebook have a range of privacy settings that are often set up to 'expose' your details to anyone. When 'open' anyone can find you from a search of the social networking site or even from a Google search. Therefore, it is important to change your setting to 'just friends' so that your details, comments, photographs can only be seen your invited friends. Please read the following guidelines to further 'Safeguard Yourself'.

- Have a neutral picture of yourself as your profile image
- Do not post embarrassing material or comments that may call into question your employment status
- Do not accept friendship requests unless you know the person or want to accept them - be prepared for being bombarded with friendship requests from people you do not know
- Do not make friendship requests with service users
- Choose your social networking friends carefully and ask about their privacy controls
- Do not accept friendship requests on social networking or messaging sites from the children, young people (or their parents) or service users that you work with.

For those working with young people remember that ex pupils may still have friends that you may have contact with through your work

- Exercise caution. For example, if you write on a friends ‘wall’ on Facebook all of their friends can see your comment even if they are not your friend
- There is a separate privacy setting for Facebook groups and networks. You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network is able to see your profile
- If you have younger friends or family members on your social networking groups who are friends with children, young people (or their parents) or service users that you work with, be aware that posts you write will be visible to them
- Do not use your personal or professional details (email or telephone) as part of your profile
- If you or a friend are tagged in an online photo album (Facebook, flickr) the whole photo album may be visible to their friends, your friends and anyone else tagged in the photo album
- You do not have to be friends with anyone to be tagged in their photo album, if you are tagged in a photo you can remove the tag but not the photo
- You should be aware of the privacy settings on photo sharing websites
- Your friends may take and post photos that you may not be happy about. You need to speak to them first to request that it is removed rather than contacting the web provider. If you are over the age of 18, the website will only look into issues that contravene their terms and conditions
- Do not use your personal profile in any way for official business. If you are going to be a friend of your organisations official social networking group ensure you have a separate professional profile

If you have difficulty in implementing any of this guidance speak to the Headteacher.

Appendix A: Acceptable Use Policy COVID-19 Addendum

This addendum is for the period of partial school closures imposed by the Government during the Coronavirus (Covid 19) outbreak only. Any additions or amendments listed should not in any way override or diminish an individual's responsibility to safeguard children and to act in an appropriate and professional manner at all times.

Where no exceptions and amendments are stated below then it should be understood that the expectations set out in the main body of this policy and in the Acceptable Use Agreement still wholly apply.

In school

We will continue to have appropriate filtering and monitoring systems in place in across the school.

Admin staff will be available to advise staff and are continuing to monitor the systems regularly. Any concerns will be passed on to the Designated Safeguarding Lead (DSL) or one of the DSL Deputies.

Outside school

Staff should be aware that school-owned devices used in the home setting may be subject to monitoring and access to inappropriate websites or engaging in inappropriate online behaviour remains a disciplinary matter.

Where staff are interacting with pupils online, they will continue to follow the existing Staff IT Acceptable Use Agreement, and adhere to guidance in the Safer Working guidance https://www.safeguardingchildren.co.uk/wp-content/uploads/2020/04/Guidance-For-Safer-Working-Practice-COVID-addendum-April-2020.pdf

as well as the current Safeguarding Online Safety Policies. In these policies, clear guidelines are set out for the Safe Use of School IT equipment and the school network in relation to communicating with pupils and appropriate use of language.

As per this policy, staff continue to be prohibited from using social networking sites or apps to communicate with pupils, other than sites or apps approved by the Headteacher and used to communicate with the whole school or parent community.

Any professional communications whether sent from a school or personal device in the course of a member of staff's duties may be used as evidence should any disciplinary procedures commence as a result of breaches of this or any other policy.

Pupils are unlikely to be using a filtered internet connection at home, so staff should be alert to signs that pupils may be making inappropriate use of the internet through comments they make or posts they share. Any concerns should be shared with the DSL in the usual way.

Pupils know how to report any concerns they have back to their respective school via email to their form tutor or head of year.

Working with parents and carers

We will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online
- Know what our schools are asking children to do online, including what sites they will be using and who they will be interacting with.
- Know where else they can go for support to keep their children safe online

Throughout the closure, regular updates will be offered to parents including links to relevant websites / media for further guidance.

Email and Internet Use

We appreciate that we are operating in extraordinary times where many members of staff will often be working from home and may be using their own devices for contacting pupils but staff should be

reminded that all clauses of our Acceptable Use Policy still apply when engaged in any communication with pupils, colleagues, parents and other stakeholders.

Staff are reminded that all aspects of GDPR and the Data Protection Act 2018 apply. Please pay particular attention to emails and other forms of communications and make sure:

- they are only sent to intended recipients
- they are purposeful and professional
- any emails addressed to multiple recipients use the BCC function so that, for example, parents' email addresses are hidden. Ideally, communications sent to multiple recipients such as a tutor group or year group will be sent by such proprietary methods as *SchoolComms*.
- At no time should any school business be conducted using a personal email address.

Other GDPR and professional conduct points to be reiterated at this time include:

- Staff may have access to special category personal data about pupils and their families which must be kept confidential at all times and only shared when legally permissible to do so and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.
- Staff should never use confidential or personal information about a pupil or her/his family for their own, or others advantage (including that of partners, friends, relatives or other organisations). Information must never be used to intimidate, humiliate, or embarrass the child.
- Confidential information should never be used casually in conversation or shared with any person other than on a need-to-know basis. In circumstances where the pupil's identity does not need to be disclosed the information should be used anonymously.
- Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries.

Mobile Phones and Other Electronic Devices

If the use of a personal mobile device is unavoidable for contacting a parent/carer, then the number must be withheld, e.g. by typing 141 before dialling the parent/carer number. Staff personal mobile numbers should never be given to pupils or parents.

All email contact with pupils must be made using the member of staff's and the pupil's school email address, or through Microsoft Teams.