Staff Policy on the use of Information Communication Technology, including Computers, Email, Phones, Internet and Social Media

1 Introduction

1.1 This policy covers all forms of Information Communication technology, in all hardware, software and electronic forms.

1.2 Technology, including the internet, is vital to our activities and increasingly we are reliant on e-mail as a method of communication and the internet as a tool for information and research, and for communication with service users and partner organisations. However, it is important that all users access and use this technology appropriately and responsibly. This policy aims to outline what misuse is, how to avoid such abuse and to ensure that access to technology is an asset and not a liability to individuals and the organisation.

1.3 Definitions:

1.3.1 The term 'IT resources' is used throughout this policy. This term covers any hardware, including desk top computer, laptop, tablet or smart phone at our place of work or for remote working from home or another venue and use of the e-mail and internet facility. It also covers any software, communications systems, and internet activity.

1.3.2 The Term "manager" refers to an individual's line manager.

1.4 This policy applies to all staff, and any volunteers or Board members who have access to North Halifax Partnership (NHP) ICT systems or resources.

1.5 Any breaches of this policy or abuse of IT resources, will be considered as a disciplinary matter. Some breaches may be considered as incidents of gross misconduct.

2 Acceptable and Unacceptable computer use

2.1 All staff must comply with the Internet and Email Acceptable use rules which are set out in this policy. The following examples will be considered as unacceptable use of IT resources:

2.1.1 Personal or recreational use (See Section 5)

2.1.2 Any purposes that would damage the organisation’s reputation

2.1.3 Perpetrate any form of harassment

2.1.4 Viewing, exchanging or producing unacceptable material. This includes pornographic, violent or hateful material

2.1.5 For gambling

2.1.6 Any illegal purpose

2.1.7 Intentional ‘hacking’ of IT systems (NHP’s or others)

2.1.8 Undertake work for other employers or for own business/commercial purposes

2.1.9 Knowingly downloading, sharing or distributing software, files or other material that breaches Copyright laws.

2.1.10 Taking photographs of children or service users or any other persons you meet during the course of your work on a personal device.

2.1.11 Downloading applications to a work device that are not necessary or required for work purposes, this includes apps relating to social media.

2.2 An Internet Acceptable Use Quick Reference Guide is enclosed in **Appendix 1**.

3 Use of Calderdale Council Intranet

3.1 Some NHP staff have access to Calderdale Council’s intranet. In recognition of this staff must ensure that when browsing this facility any documents downloaded from the site are for internal use only and are not to be copied and / or distributed within the public domain. It is extremely important that this rule is rigorously observed given the confidential nature of the some of the information contained within the site. The only exception is where information is already available to the public at www.calderdale.gov.uk. Where a member of staff is unsure then they should seek the advice of their line manager in the first instance. (TUPE staff will be on a different network and will not be able to access this area)

4 Use of portable electronic devices: remote and mobile working

4.1 At no time should any portable device (such as Laptop, USB/ “memory stick”, smart phone) be connected to the organisation’s IT network unless that device has been provided by Calderdale Council or NHP specifically for work use; and has been encrypted.

4.2 You should contact your line manager if you foresee a need for an encrypted portable device.

4.3 Personal laptops and tablets can be used to undertake remote working, as long as permission has been given by a line manager that the device is suitable for remote working. Please refer to the Remote Working Policy.

4.4 You must **never** download work documents onto an unencrypted portable device, or personal device; and wherever possible avoid carrying any sensitive data and information on a portable device.

4.5 Personal mobile phones should only be used for work purposes where express permission has been given by a line manager.

4.6 Personal contact details relating to service users may be stored on mobile phones provided the device is password protected so that unauthorised access is prohibited.

5 Reasonable personal usage

5.1 Nearly all employees have access to IT resources, therefore NHP recognises that a small amount of personal usage is acceptable. This is so long as personal usage does not incur a cost, is moderate and does not interfere with the individual's usual duties (or those of others).

5.2 Users are not permitted to spend excessive time online or surfing the internet and personal use during working hours.

5.3 Staff who have access to a business mobile phone are permitted to use their work phone for personal usage in line with the agreement at Appendix 4.

5.4 Any personal use that conflicts with the code of conduct will be treated as a disciplinary issue.

5.5 Storing personal data on NHP devices is not permitted. This includes storing personal photographs or personal contact details.

6 Personal devices

6.1 For day-care staff, personal mobiles should be stored in individual lockers or other agreed place for personal belongings

6.2 Personal mobiles must not be used for private calls during contact time with children/families or in meetings, unless this have been discussed and agreed with your line manager beforehand. Mobile phones should be switched off or on silent during these times.

6.3 Personal mobiles may be used in designated staff areas (indicated in each workplace) but you must not switch them on in any room where there are children or service users. You must finish your conversation (including text messaging) before returning to an area where there are children or service users.

6.4 In exceptional circumstances, staff that do not have a work mobile may be asked to ensure they have their personal mobile available to use in case of emergency. This will always be documented in the risk assessment for the activity such as an outing with children and service users. This also applies to staff that have hybrid working agreements and do not have an NHP device.

6.5 You should avoid using your personal mobile to contact service users as far as is possible. In exceptional circumstances personal contact details may be temporarily stored on your personal mobile phone, but only where:

- You have been given permission by the data subject (see data protection working practice); and
- The device is password protected so that unauthorised access is prohibited.
- These details should be deleted as soon as practical.

7 Use of mobile phones in the workplace

7.1 The use of mobile phones by staff and service users (including parents) is restricted in most NHP workplaces, principally to safeguard children and other service users. Each Family Hub has specific information for parents about this, and staff must explain these requirements to parents. Staff should also ensure they follow any provisions set down in risk assessments for specific events. See **Appendix 2** -*Statement for parents about phones and photos.*

7.2 All staff should be mindful to advise service users and other people about their use of mobile phones when attending meetings, home visits and other NHP events organised by NHP – where this is reasonable and appropriate. If in doubt, ask your manager, but please bear these factors in mind:

7.2.1 In Family Hubs we do not allow parents to take any photos of their children

7.2.2 Most people nowadays will recognise why you might ask them not to take photos – especially if you are going to produce some which they can share.

7.2.3 Some meetings are very contentious and it can accelerate the tension if someone is recording them on a phone or other device. Try to gain the confidence of people at the meeting that the note will be accurate and shared with all present, and that recording is therefore not needed.

7.3 Staff may log on to Wi-Fi at their home addresses to save on data usage – please refer to the Remote Working policy.

7.4 Staff are not permitted to log any NHP device to public Wi-Fi for purposes of remote working.

8 Social Media and Social Networking

8.1 Social media includes online social forums such as “X”, Facebook and LinkedIn. Social media also covers blogs and video and image-sharing websites such as YouTube and Flickr as well as ‘closed/secret’ forums where information is exchanged between a specific group of people. IT based social networks are part of a mass media and privacy cannot be guaranteed. Whilst you may believe that you are communicating privately with a friend, relative, neighbour or work colleague , you cannot control what they do with that information or guarantee that the information will not be passed on to others. Any breach of what you thought was a private exchange need not happen maliciously and the person you thought you had privately communicated with may not feel it is a breach of confidence if they pass the information on to another friend of theirs who doesn’t even know you. The passing on of information could even happen by mistake or so to speak by someone ‘pressing the wrong button’.

8.2 When you write something down, or in this case type something from your computer, and then pass it to others then you leave yourself open to accusations of defamation, which in the case of the written word is libel. If someone believes what you have said about them is untrue then they can sue you for defamation and in which case the onus in court is on you to prove what you have said is true.

8.3 All staff and volunteers are bound by the NHP code of conduct, which includes behaving in a manner which maintains the integrity of the organisation. Staff must not undermine the programmes, their own position or that of their colleagues at work or off duty. In respect of Facebook and other social networks – whenever used - this means that all staff must:

8.3.1 Comply with the instructions below; and

8.3.2 Understand your online **privacy** settings – check your settings and understand who can see the information you publish and your personal information. There has been a rise in identify theft and fraud and consideration should be given to the amount of personal information that is displayed on your personal profiles.

8.3.3 Ensure there is nothing in your online profile that is inconsistent with the NHP Code of Conduct and/or Equality and Diversity Policy:

8.3.4 Ensure you make no communication in a personal capacity which

- Brings NHP into disrepute
- Breaches confidentiality

- Could be considered as discriminatory against, or bullying or harassment of any individual.

8.3.5 Never discuss any aspect of your work, including working relationships on Facebook or any other social networking site.

8.3.6 Never use personal accounts on Facebook or other social networking sites as a medium for any aspect of your work. Use of NHP, Family Hubs Facebook Accounts is directed by the Service, the Comms team and the Neighbourhood Manager.

8.4 You may become aware through a third party, or in your personal time, of something on Facebook or another social networking site which you feel is relevant to our work. This could include information about anti-social behaviour or crime at one end of the scale. At the other end of the scale, you could spot an opportunity to promote our work. This does not affect the instructions at 8.3 above.

8.4.1 If you have something to communicate and you are not sure about how to do it, please speak to your line manager or volunteer supervisor.

8.4.2 Never trawl social networking sites for intelligence. If you become aware of information via a social networking site that you think the police or safeguarding agencies should be aware of, speak to your line manager or volunteer supervisor.

8.4.3 Do not download and email extracts from social networking sites unless specifically asked to do so by your manager on behalf of the Police.

9 Data protection issues and e-mail communication

9.1 The NHP Data Protection Policy, NHP Privacy Notices and associated working practices set out how the organisation protects personal data of staff, service users and stakeholders. You should take particular care when using mailing lists, that the people on that mailing list have given you explicit consent to contact them in this way.

9.2 In addition to the provisions of paragraph 2.1 above, and the information found below, all staff should follow these instructions:

9.2.1 **Do not** email pictures of anyone to anyone else (unless they have been subject to a consent form)

9.2.2 When you send emails to members of the public, or mailing lists that include members of the public, **Do not** put the resident or service users email addresses in “To” or “CC” line. They must always go in the Bcc box. If you are sending an email to more than one resident or service user, get a colleague to double check that you've got them in the right box before you send.

9.2.3 Care should be taken when circulating emails containing personal details about an individual. E-mail both internal and external mail is not a secure method of sharing personal information about any individual adult or child. It is acceptable to send information by email if it only contains one identifier about an individual – e.g. a register for a training course with only names. If you send more than one piece of personal information – for example name and date of birth this must either:

- Be sent in a password protected file by email with a password separately notified by phone or in person to the person for whom the data is intended: or
- Be produced as a hard copy and delivered to the organisation involved.

9.2.4 Great care should be taken when opening e-mails from unknown sources as they may contain offensive messages or images or may contain a virus. If you have a doubt as to whether an e-mail is appropriate to open please ring seek advice from the IT Helpdesk, or consult your manager or volunteer supervisor If you realise later that you have opened, and /or responded to an inappropriate or hoax email, tell your line manager or volunteer supervisor immediately. Staff should not partake in sending so called 'chain mail' and any chain mail messages received should be deleted immediately.

9.2.5 It is accepted that an individual may unknowingly or unwittingly (eg pressing the wrong button) open an e-mail or website that contains material that would be in breach of this policy. In that situation please advise your manager at once and this will not result in disciplinary action. However, if you fail to report such an action you may not be protected if it is subsequently discovered that inappropriate material has been accessed/downloaded on your computer.

10 **Cameras and photographs**

10.1 Only cameras/devices that are provided by NHP should be used to take photographs. Personal cameras must not be brought into the workplace and taking photographs on personal devices is strictly forbidden.

10.2 You should use the camera/device provided; and follow the instructions in respect of consent for, use of, and storage of the images taken. See

Appendix 3 below for principles. Detailed working practice about consent, storage and use of images sits with Data Protection Policy

10.3 Family Hub devices must not be taken from the premises unless authorised by the responsible person and will only be used out of the centre in exceptional circumstances. Other devices (e.g. for family support and community engagement teams) will be used more frequently outside the work base and must be signed in and out of the building.

10.4 All images should be deleted from the device as soon as you have saved or printed those images you need. Images taken by NHP staff should be stored within whichever centre, team or project folder is appropriate in a clearly marked sub-folder.   See **Appendix 3** below for principles. Detailed working practice about consent, storage and use of images sits with Data Protection Policy

11 Responsibilities – Virus and Spam

11.1 In addition to the privacy and Data Protection instructions above. When using IT resources, including emails, users should:

- Not open e-mails or data files that is in a format, or comes from, a source that you do not recognise. Do not open the item and contact the IT support team for advice.
- If you receive any unsolicited e-mails or spam that manages to bypass the IT spam software, you must not respond in any way. Some spam e-mails may offer the option to opt out of receiving them. Be aware that this is sometimes used as a way by unscrupulous spammers of validating a live e-mail address.
- You must take all reasonable actions to ensure that the Company is protected from viruses. Measures include:
    - checking the source of emails.
    - not opening emails where the source is not recognised or appears suspicious.
    - not clicking links or opening attachments in emails, where the sender is not known.
    - seeking advice from IT support at the earliest opportunity.

11.2 The data allowance on each work phone may be used to access sites (e.g. Job Centre Plus) or to download apps that support their work with service users. (e.g. satellite navigation). Individuals must check with Business Support Manager before installing other apps.

12 Harassment

12.1 The NHP code of conduct requires all staff and volunteers to treat colleagues with dignity and respect. Any form of harassment, intentional or not, will be treated as a disciplinary matter.

12.2 Any communications that are considered to be sexist, racist or contain offensive material or remarks could be considered unlawful harassment and will be treated as such.

12.3 Any form of 'cyber-bullying', that is to use electronic communication or IT resources as a means to intimate or bully colleagues will not be tolerated. This is irrespective of whether communication is made through business or personal accounts.

13 Freedom of Information Issues and email communication

13.1 From time to time, our services may be required to supply written information for members of the public, under the Freedom of Information Act. Under the Act, recorded information includes emails and file notes relating to the information requested. Staff should remember this is another reason to ensure all their emails are professional in nature, and comply with Data Protection principles.

14 Your obligations under the NHP whistle blowing policy

14.1 If at any time you are concerned about a colleague's conduct in relation to email and computer use (this includes external organisations, volunteers and clients), you must report this immediately to your line manager or volunteer supervisor. See the whistleblowing policy for further information.

15 Security

15.1 It is the employee's responsibility to use only their own ID and password when accessing the organisation's IT resources. Passwords and access codes must not be shared with others, inside or outside the organisation.

15.2 Passwords must be changed when prompted.

15.3 Issue and queries including permission to reset the pin which locks the phone should be directed to Business Support Manager (Diane Coenen), or in her absence Payroll Officer (Kim Connell).

15.4 Lost or stolen work mobiles should be reported as above if the loss happens on a weekday. At weekends, contact the provider on 07953 966150, then report to Business Support Manager on the following Monday.

15.5 Mobile phone users will sign the contract in **Appendix 4** to confirm safe receipt of the device.

16 Monitoring

16.1 In order to monitor this policy your manager or volunteer supervisor reserves the right to access your computer. You are assured that such access would be exceptional other than for normal business use. However, you should also be aware that the Council's ICT service performs regular and random sweeps of email and internet usage and will investigate any suspected misuse, which could lead to disciplinary action, and /or prosecution

The purposes for such monitoring are to:

- promote productivity and efficiency
- ensure the security of the system and its effective operation
- ensure there is no unauthorised use of the Company's time, e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications.
- ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked
- ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- ensure that inappropriate websites are not being accessed by employees
- ensure there is no breach of confidentiality or Data Protection.

NHP Internet Acceptable Use   Quick Reference Guide

Key messages

- The internet facilities provided by NHP are made available for its business purposes
- You may use the internet in your own time (for example during your lunch break) if no one else needs your computer
- You are responsible for the security provided by your network account logon-id and password; and you must not divulge these to any other person, or allow any other person to use your account.
- You must not create, download, upload, display or knowingly access, sites that contain pornography or other materials that might be deemed illegal, obscene or offensive
- Your internet activity is recorded and monitored.

Failure to comply with this Policy document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police

Appropriate Usage

✓ Use of internet facilities for work purposes

✓ Use of internet facilities for personal purposes outside work times if no one else needs your computer

✓ Use of internet facilities with the prior approval of your manager for personal purposes in work time

"Work time" means any time you are working for NHP – not just core hours or "office" hours

Inappropriate Usage

The list below gives examples, but it is neither exclusive nor exhaustive. "Inappropriate" material includes all data, images, audio or video files the transmission of which is illegal under British law, and all material which is against the rues, essence and spirit of this and other NHP policies

Do Not Allow:

× Anyone else to use your internet access or provide any person with the means to access these facilities

Do Not Attempt:

× To gain unauthorised access to (hack) any server/facility whether inside or outside the NHP or Calderdale Council

Do Not

× Use web-based email service such as Hotmail for NHP business purposes except by the express permission of the Service or Neighbourhood Manager for specific projects

× Subscribe to or enter or utilise real time chat facilities except by the express permission of the Service or Neighbourhood Manager for specific projects× Enter or use peer – to-peer networks or install software that allows sharing of music , video or image files

Do Not Download:

× Any unauthorised programmes/software, such as screen savers, onto NHP or Calderdale Council ICT equipment

× Any personal media such as personal music tracks, video, images etc onto the NHP or Calderdale Council ICT equipment

Do not knowingly:

- ✗ Create, download, upload, display or access, material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone else who sees the material, harassment, alarm or distress.
- ✗ Use the facilities for any activity which is illegal or fraudulent
- ✗ Engage in any activity which threatens the integrity or availability of the NHP's or Calderdale Council's systems
- ✗ Infringe copyright or intellectual property rights

Do not use the

- ✗ Facility to pursue personal business interests, including sale of goods and services, gambling, or for political purposes not directly related to your job
- ✗ Facilities to upload to any external website PROTECT or RESTRICTED or Confidential material concerning the business/activities of the NHP or Calderdale Council.
- ✗ Facility for personal purposes in work time UNLESS usage is in compliance with the Green Acceptable Use in Section above

"Work time" means any time you are working for NHP – not just core hours or "office" hours

Appendix 2

Safeguarding Statement for parents and carers:

taking photos of children using Family Hub Services and using mobile phones in sessions

NHP takes very seriously the need to safeguard children attending any activity organised by our staff.

Our policy, after consultation with parents, is that parents should not use their phones or cameras to take photographs of any children - including their own - when attending activities at the Family hub for any purpose including placing on Social media, for example FaceBook or "X".

Staff running activities will challenge any parents seen to be doing this.

Each Family Hub has a camera/device and staff can, if asked, use this to take photos as appropriate.

The Family Hub will then arrange for the parent to have a copy.

We appreciate that while using the Family Hub sometimes you may need to answer your mobile phone or send a message in an emergency. We ask that if you need to do this you be as discreet as possible and if you need to speak on the phone you go out of the room whilst you take the call and ask someone to watch your child for you.

Thank you for your cooperation in this matter.

Appendix 3

Guidance on storing photographs: Principles

(See Data Protection Working Practices for NHP Photo Consent form, and detailed guidance Table on consent, storage, and use of images)

- Ensure you give each image a descriptive file name and date (eg *Boy with tea set KPCC March 2020*).
- Do not save multiple pictures of the same thing. As a rule of thumb – aim for no more than 6 images for each event/" photo shoot".
- Each month, all photographs which are 6 months old or more should be deleted. You may keep older photographs in hard copy and secure files for OFSTED evidence if agreed with the senior manager of your hub or team.
- All displays which include pictures of children and service users must be refreshed every 6 months, and the pictures disposed of securely.
- Images specially commissioned by professional photographers and film makers will be saved in Shared drive and may be kept for up to 3 years – depending on the written particulars of original consents.
- No image older than 6 months should be stored on the Shared drive

Consent for images/photos – see Data Protection Working Practices

- You must gain and record the express and written consent of the child's parent/carer in the case of children; or adult service user /data subject before taking any photograph. Methods to gain written consent include registration document at NHP nurseries; meetings and events signing – in registers; photo consent forms for specific photo shoots, films etc. and events where there is no register to sign.
- Any person working in partnership or under contract to NHP (for example family learning tutors) must also gain express consent to take and use images. This must be discussed in advance with relevant NHP staff, and any agreement made, be recorded in writing.

Appendix 4

[date]

Re: Staff Contract Phones

This mobile phone is issued to (insert staff name), (insert job title) whilst working for NHP Limited.

All personal calls have to be paid for. Staff may not use their mobile phone for personal use unless absolutely necessary.

Whilst the mobile phone is in your possession you are responsible for its safe keeping. Loss or theft of a mobile phone must be reported immediately to either your line manager or the Business Support Manager in order for the account to be closed and the service stopped. The phone remains the property of NHP Limited.

Your phone should be used in line with the staff use of computers policy, and should not be used to access social media sites etc. It should also not be connected to any PC.

Type of phone –

Serial number –

Puk number –

Telephone number -

Signed ___________________________________Date ______________________

Diane Coenen on behalf of NHP

Signed ___________________________________Date ______________________

(staff name), (staff job title)