E-SAFETY POLICY

DOCUMENT PURPOSE

This policy reflects the National Institute's values and philosophy in relation to E-safety. It sets out a framework within which staff, volunteers and students can operate to keep children safe when using technology, especially the internet.

SCOPE OF POLICY

This policy applies to all members of NICE (including staff, students, volunteers, parents/carers, visitors) who have access to and are users of NICE ICT systems, both in and out of the Institute.

This policy document has been developed and agreed by the whole staff. A copy of the document is kept in the School Policy Document File, which is kept by the Children's Services Administrator. This central location ensures the accessibility of the document to visiting teachers, for example outreach or support teachers, and parents. Copies of the document are also available from the CEO. Staff have access to this policy via the W drive on the server.

The term staff in this policy will relate to anyone who is employed at NICE. The term student will relate to those studying any course provided at NICE or take up a work experience placement. The term pupil refers to the children in School Group and Pre-school.

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within NICE.

GOVERNORS:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular information about e-safety incidents and monitoring reports from either the Designated Safeguarding Lead or the E-Safety Coordinator.

DESIGNATED SAFEGUARDING LEAD:

The Designated Safeguarding Lead (Marie McCann) should be trained in e-safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Takes a day to day responsibility for e-safety issues and will lead on e-safety issues
- Will report e-safety incidents to the Governors
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place

E-SAFETY COORDINATOR:

The E-Safety Coordinator (Maryum Raja) is responsible for the following:

- Has a leading role in establishing and reviewing the institute e-safety policies/documents
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Will report e-safety incidents to the Governors
- Monitors software on the School Group and Pre-School computers and are updated when necessary
- Will deliver e-safety sessions to the children to ensure they are aware of the dangers online
- Making sure that children have access to age appropriate e-Safety curriculum, which promotes their ability to use technology responsibly whilst being safe online and keeping others safe

NETWORK MANAGEMENT COMPANY:

The Network Management Company is responsible for ensuring:

- That the technical infrastructure at NICE is secure and is not open to misuse or malicious attack
- That users may only access the network and devices through a properly enforced password
- That users only have access to relevant folders relating to their work
- The software on the connected computer terminals are updated when necessary

STAFF:

Staff across the whole organisation are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (see Appendix A)
- They report any suspected misuse to the CEO/Designated Safeguarding Lead for investigation/action
- All digital communications with students/participants/parents/carers/community members should be on a professional level and only carried out using the Institute's systems

STUDENTS:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement (appendix B)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand the restricted use of mobile devices and digital cameras when around Children's Services and Adult Rehabilitation Services
- Should understand the importance of adopting good e-safety practice when using digital technologies out of NICE and realise that this policy covers their actions off these premises, if relating to their membership of NICE

E-SAFETY FOR CHILDREN'S SERVICES STAFF:

Staff within these departments also have the responsibility to ensure that:

- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use agreements
- They monitor the use of digital technologies, mobile devices, cameras in lessons and other school activities and implement current policies with regard to these devices
- In lessons where internet use is pre planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

PARENTS/CARERS:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. NICE will take every opportunity to help parents/carers understand these issues through informal discussions, newsletters and specific e-safety workshops. They also receive a letter detailing e-safety rules at the beginning of each academic year.Parents and carers will be encouraged to support Children's Services in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to the children's Seesaw Profiles

EMAIL

The use of the internal e-mail system and use of the Internet within NICE is encouraged, as its appropriate use facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees.

- Before being able to use the internal email system or internet staff are required to sign the Email and Internet Use Agreement which forms part of the Staff Acceptable Use Agreement
- All staff have access to their work email on the server. They will only be able to access this by using their correct log in information
- The official institute email service may be regarded as safe and secure and is monitored. Users should be aware that email communications can be monitored
- Users must immediately report, to the E-Safety Coordinator, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication sent from the work email must be professional in tone and content
- Staff are able to check their work email remotely using an IP address. The pupils in School Group also have a joint email account for correspondence with pupils that have left the school or attend on a fixed term basis. Emails are checked by School Group staff who help them to respond

SOCIAL NETWORKING

The term '**blog**' is short for 'web log'. A blog is an online diary detailing personal insights and experiences. This is shared with an online audience.

A **Social Network Site** is a website, which allows individuals to construct a public or semi-public online profile and to connect with others who share similar interests and views.

STAFF (INCLUDING VOLUNTEERS AND STUDENTS)

NICE recognises that blogs and social networking sites provide a useful tool for communication and are accessed widely by many employees. (Therefore, NICE does not restrict access to these sites.)

Employees may access personal blogs/social networking sites on work premises for their own use, provided that this is outside of working hours (agreed for each section//team/individual), is not excessive, and observes the restrictions outlined below (this information can also be found in the Social Networking Use Agreement. Appendix C).

Staff must not:

- disclose any information that is confidential to the Foundation or any third party or
- disclose personal data or information about any individual/colleague/service user, which could be in breach of the Data Protection Act 2018;
- disclose any information, which is not yet in the public arena;
- post illegal material, e.g. images of child abuse or material which incites racial hatred:
- link their own blogs/personal web pages to the Foundation's website;
- include any information, sourced from the Foundation, which breaches copyright;
- make defamatory remarks about the Foundation, colleagues or service users;
- publish any material or comment that could undermine public confidence in you as an employee/Student of the Foundation and/or in position of trust within the community; and/or
- misrepresent the Foundation by posting false or inaccurate statements about the work of the Foundation.

USING SOCIAL NETWORKING SITES TO ENGAGE WITH COMMUNITIES

Some staff at NICE need to communicate and engage with other organisations / groups as part of their work. Social networking sites represent an opportunity for such engagement.

However, there are risks associated with using these sites and employees wishing to use this method of engagement, should ensure they have thought about the potential risks involved.

SOCIAL NETWORKING SITES IN CHILDREN'S SERVICES

Social networking sites such as Facebook, Twitter, or Instagram have a minimum age of 13 years and therefore are not used, mentioned or glorified during the school day.

Pupils in School Group and Pre-School are now using Seesaw: The Learning Journal to record the work that they do during the school day. This is shared directly with the parents and other relevant school placements and professionals (with the written consent of parents) who are given a unique QR code to link up to their own child's profile. The pupils use a picture of an animal as their 'profile picture' and only appears along-side their first name.

WORLD WIDE WEB

- If staff, students or pupils discover unsuitable sites, the URL (address), time, content must be reported to the E-Safety Coordinator and IT Coordinator who oversees IT provision for Children's Services
- School will ensure that the use of Internet or digital world derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- All sites that are accessed during lessons should be tested by staff to ensure that all content is relevant prior to the lesson/activity
- When conducting research using the World Wide Web pupils will use either www.safesearchkids.com or www.kidrex.org as they are both safe search engines designed for children by Google

FILTERING

NICE uses Endpoint Security Console on all staff terminals which is monitored and maintained by EBC. Terminals are further secured by the Webroot Filtering Extension when accessing the internet via a web browser.

The classroom based computer in Pre-School has K9 web protection installed to ensure filtering systems are as effective as possible. This is monitored and updated when necessary. In School group the secondary computer is installed with K9 web protection however, the main computer does not have K9 web protection installed as it is only accessed by members of staff. YouTube is used on this computer but it is signed in to the restricted mode.

BRING YOUR OWN DEVICE (BYOD):

There are many educational and social opportunities offered by mobile technologies which are being expanded as a wide range of devices, software and online services within and beyond NICE. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include: levels of secure access, acceptable use, support, auditing and monitoring.

- NICE has a set of clear expectations and responsibilities for all users
- NICE adheres to the Data Protection Act 2018 principles
- All users are provided with and accept the Acceptable Use Agreements
- All network systems are secure and access for users is differentiated
- These devices will only be connected to the Wi-Fi
- Students receive training and guidance on the use of personal devices

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff, and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, and parents/carers need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. NICE will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students and pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached with publishing their own images on the internet e.g. social network sites and Seesaw: The Learning Journal.
- Parents and carers are welcome to take videos and digital images of their children at NICE events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupil's in the digital/video images.
- Staff can take digital/ video images to support educational aims, but must follow NICE policies concerning the sharing, distribution and publication of those images. Those images should only be taken on equipment owned by NICE, the personal equipment of staff will not be used for such purposes.
- Pupils must not take, share, or publish images of others without their permission.
- Photographs published on the website, or elsewhere that include participants and pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Participants and pupils full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained at the beginning of each academic year before photographs of pupils are published on the NICE website.
- Pupils work can only be published with the permission of the pupil and parents or carers.

NICE WEB SITE

- The contact details on the Web site are the institute address and telephone number. Staff, participants' or pupils' personal information will not be published
- The pupils in School Group and Pre-School have access to Seesaw: The Learning Journal on the iPad's where they can publish their work (pending acceptance from the app administrator) for their parents (and relevant other school placement) to see. All pupils have their own separate profiles with a secure QR code log-in

PROTECTING PERSONAL DATA

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data and "locked" if planning to return to the computer
- Transfer data using encryption and secure password protected devices
- Documents from Local Authorities can be securely sent to us using Egress. These are sent to our Administrator who has access
- Pictures and data are automated to be deleted at the end of each academic year to protect present individuals and those who have left

Review Frequency: Annually **Next Review:** January 2022

APPENDIX A

STAFF ACCEPTABLE USE AGREEMENT

AUTHORISED USE

The internal e-mail system and use of the Internet are available for communication on matters directly concerned with the business of the Foundation. Employees using the e-mail system should give particular attention to the following points.

1. The standard of presentation. The style and content of an e-mail message must be consistent with the standards that the Foundation expects from written communications. If a member of staff is unsure of the standards required they should approach their line manager.
2. The extent of circulation. Internal E-mail messages and external messages via the internet should only be sent to those employees for whom they are particularly relevant.
3. The appropriateness of internal e-mail. E-mail should not be used as a substitute for face-to-face communication. "Flame-mails" (e-mails that are abusive) can be a source of stress and damage work relationships, and also be used in a disciplinary or grievance procedure. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.
4. The visibility of internal e-mail. If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality, or perhaps communicate the message in some other way.
5. E-mail contracts. Offers or contracts transmitted via e-mail are as legally binding on the Foundation as those sent on paper.

UNAUTHORISED USE

Any failure to follow these guidelines satisfactorily can result in disciplinary action.

6. The Foundation will not tolerate the use of the internal/external system for any of the following:

    - any messages that could constitute bullying or harassment (e.g. on the grounds of sex, race or disability);
    - on-line gambling;
    - accessing pornography;
    - downloading or distributing copyright information and/or any software available to the user;
    - posting confidential information about other employees, the Foundation or its customers or suppliers:
    - inappropriate use of social networking sites (please see separate policy for further details)

Any unauthorised use of internal e-mail or the Internet is likely to result in disciplinary action.

IMPLEMENTATION OF THE POLICY

7. All new employees will be trained on how to use the internal e-mail system and internet. If any member of staff is experiencing difficulty with either system then they should inform their line manager immediately.

8. All internal e-mail users will be issued with a unique individual password which is confidential to the user, and may be changed if a member of staff feels that other members of staff know their password (see the Support Services Manager in order to do so). Access to the internal e-mail system using another employee's password without prior authorisation is likely to result in disciplinary action.

9. Users must ensure that critical information is not stored solely within the internal e-mail system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

10. Users are required to be familiar with the requirements of the Data Protection Act 2018 and to ensure that they operate in accordance with the requirements of the Act and ensure that they adhere to the Data Protection Policy that the Foundation holds.

11. Employees who feel that they have cause for complaint as a result of internal e-mail communications should raise the matter initially with their immediate line manager and/or the Support Services Manager. If necessary, the complaint can then be raised through the grievance procedure.

I ..... have read and understood the above information and agree to the appropriate use of the Internet and Foundation email.

Signed.....

Date.....

APPENDIX B

STUDENT ACCEPTABLE USE AGREEMENT

Digital technologies have become integral to the lives of students, both within educational settings and outside these settings. These technologies are powerful tools, which open up new opportunities for everyone.

THIS ACCEPTABLE USE POLICY IS INTENDED TO ENSURE:

- That students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- That NICE systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

NICE will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

This policy applies across the whole network and includes WiFi.

Your activity on the internet can be closely monitored by NICE, logs can be kept of activity through the use of your own device through the WiFi at NICE.

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use NICE ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

FOR MY OWN PERSONAL SAFETY:

- I understand that NICE can monitor my use of the systems and digital communications
- I will not disclose or share personal information about others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages to the E-Safety Coordinator (Marie McCann)
- I will not take pictures or videos of staff, children or participants with my own device

I understand that everyone has equal rights to use technology as a resource and:

- I will not abuse the systems provided at NICE by downloading or uploading large files that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use NICE systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting, unless I have permission and it is relevant to my studies

I RECOGNISE THAT NICE HAS A RESPONSIBILITY TO MAINTAIN THE SECURITY AND INTEGRITY OF THE TECHNOLOGY IT OFFERS ME AND TO ENSURE THE SMOOTH RUNNING OF NICE

- I understand that if I use my own devices at NICE, I will follow the rules set out in this agreement
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the security/filtering systems in place to prevent access to such materials
- I will only use social media sites outside of lecture times and when not in the presence of the children or participants

WHEN USING THE INTERNET FOR RESEARCH, I RECOGNISE THAT:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

I understand that I am responsible for my actions at NICE:

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action

I ..... have read and understood the above information and agree to the appropriate use of the Internet and Foundation email.

Signed.....

Date.....

APPENDIX C

SOCIAL NETWORK USE AGREEMENT

This document outlines the NICE's approach to blogs and details the ground rules for employees/students and volunteers who should ensure that the content of their blogs/social networking sites does not bring the Foundation into disrepute or breach their obligations under the staff handbook as employees of the Foundation.

GROUND RULES FOR EMPLOYEES

The Foundation recognises that blogs and social networking sites provide a useful tool for communication and are accessed widely by many employees. (Therefore, NICE does not restrict access to these sites.)

Employees may access personal blogs/social networking sites on work premises for their own use, provided that this is outside of working hours (agreed for each section//team/individual), is not excessive, and observes the restrictions outlined below.

Employees must also ensure they are compliant with any rules set out in the

Foundation's Internet Policy and staff and student handbooks.

Employees are advised not to write about their work or make reference to the Foundation on external web pages, i.e. in blogs or on social networking sites. Where an employee chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the foundation. In addition he/she should adhere to the rules below.

Failure to adhere to these rules may be considered misconduct and could lead to disciplinary action being taken under the Foundation's Disciplinary Procedures, which may result in dismissal.

EMPLOYEES MUST NOT:

- disclose any information that is confidential to the Foundation or any third party or
- disclose personal data or information about any individual/colleague/service user, which could be in breach of the Data Protection Act;
- disclose any information, which is not yet in the public arena;
- post illegal material, e.g. images of child abuse or material which incites racial hatred:
- link their own blogs/personal web pages to the Foundation's website;
- include any information, sourced from the Foundation, which breaches copyright;
- make defamatory remarks about the Foundation, colleagues or service users;
- publish any material or comment that could undermine public confidence in you as an employee/Student of the Foundation and/or in position of trust within the community; and/or
- misrepresent the Foundation by posting false or inaccurate statements about the work of the Foundation.

USING SOCIAL NETWORKING SITES TO ENGAGE WITH COMMUNITIES

Some employees of the Foundation need to communicate and engage with other organizations / groups as part of their work. Social networking sites represent an opportunity for such engagement.

However, there are risks associated with using these sites and employees wishing to use this method of engagement, should ensure they have thought about the potential risks involved.

MONITORING

This policy relies on Staff/Students acting responsibly and in accordance with the above rules. Where employees have concerns that colleagues are acting in breach of the above rules, they are encouraged to raise these concerns with their line manager or tutor.

Where concerns are raised these will be investigated accordingly under the appropriate procedures.

FURTHER INFORMATION

All policies and procedures form part of Foundation's employees' terms and conditions of employment and therefore care should be taken with their application.

Review Frequency: Annually **Next Review:** January 2022

I ..... have read and understood the above information and agree to the appropriate use of the Internet and Foundation email.

Signed.....

Date.....