Foundations for Children
Nursery Schools Federation

Foundations for Children Online
E-Safety Policy

Croyland Nursery School, Parklands Nursery School, Camrose Early Years Centre and Highfield Nursery School

POLICY APPROVED BY:	**Full Governing Body**
DATE PUBLISHED:	**July 2024**
DUE FOR REVIEW:	**July 2025**
TO BE REVIEWED BY:	**Cath Draper**

Foundations for Children
Nursery Schools Federation

Contents

Foundations for Children
Nursery Schools Federation

1. Introduction

This policy is relevant and applicable to all staff and Governors.
ICT and the Internet have become an integral part of our lives as well as a feature of information finding and of education. It provides our children, staff and parents with opportunities to improve understanding, access online resources and communicate with the world.

The following list identifies common internet-based technologies, which are likely to be used by young people, either at home or in an educational context:

- Websites and the use of apps (on a variety of devices)
- Social Media, including Facebook and Twitter
- Web-enabled mobile/smart phones
- Online gaming
- Learning platforms and Virtual Learning Environments
- Video broadcasting
- Blogs and Wikis
- Email, instant messaging and chat rooms and chat forums

Due to their age the majority of our children are unlikely to have been introduced to most of these applications/services. However, some may already be using them individually, whilst others may have experienced parents/carers or older siblings using them. Hence we cannot be complacent, or assume that the children will not be using technology on a regular basis, and must continue to introduce our children to ICT whilst promoting a safe use of online technologies, in the Schools and at home. Our children will begin to learn how to consider and moderate their own behaviours when using technology and begin to understand how to recognise inappropriate and unsafe behaviour in others.

As some of the technologies listed above will be utilised in the Schools, we recognise that effective policies and clear procedures for safe and appropriate use and education for staff and families about online behaviours, age restrictions and potential risks is absolutely crucial. For our safeguarding to be effective, online safety procedures must be clear, agreed and respected by everyone.

2. Why have an Acceptable Use Policy (AUP)/Online E-Safety Policy

There are risks associated with the use of on line media, and it is imperative that there are clear rules, procedures and guidelines to minimise those risks when children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail
- Grooming by people who may abuse children, usually someone pretending to be younger than their true age
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device
- Viruses
- Cyber-bullying
- Accessing on-line content, either deliberately or accidentally, which is abusive, offensive or pornographic.

2.1 Duty of Care

All schools and nurseries have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is unlikely that we will be able to eliminate them completely. Any incidents that do arise will be dealt with quickly and according to policy to ensure that the children and staff continue to be protected. The involvement of the children and parent/carers is vital to the successful use of online technologies.

2.2 The purpose of the Acceptable Use Policy

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard the children and adults. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular reviews to incorporate developments within ICT. This policy explains procedures for any unacceptable or misuse of these technologies by adults or children including:

- The steps taken in the Schools to ensure the e-Safety of children when using the internet and other related technologies.
- The Schools expectations for the behaviour of staff whilst using the internet and related technologies in and out of the Schools.

- The Schools expectations for the behaviour of staff when using ICT both professionally and socially as well as for accessing and using data.

1 *The term 'online safety' is to be used to encompass the safe use of all forms of information and communication technologies. The aim, through online safety, should be to reasonably protect all users of such technologies from potential and known risk. Technology and behaviours will be managed.*
2 *The term 'e-safety' will be used to encompass the safe use of all on-line technologies in order to protect children and adults from potential and known risks.*

3. Scope of the policy

This policy applies to all staff, children, governors, parents, visitors, volunteers and contractors accessing the internet or using technological devices on School premises. This includes use of personal devices, such as mobile phones or digital recording equipment including cameras or I-pads which are brought into the Schools. This policy is also applicable where staff or individuals have been provided with School devices for use off-site, such as school laptop or work mobile phone. The School is expected to ensure that non-employees onsite are made aware of the expectation that technologies and the internet are used safely and appropriately.

3.1 This document comprises the Federation's Acceptable Use policy, Internet policy, Camera and digital images policy, mobile phone policy and ICT Misuse policy.

3.2 This policy document should be used in conjunction with the following policies:

- Safeguarding and Child Protection policy
- Behaviour policy
- Health and Safety policy
- Technology and ICT policy
- Whistleblowing policy
- Social Networking Policy (Appendix 3)

4. Legal Background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of Schools employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act (2004)
- Working Together to Safeguard Children (2018)
- Education Act (2002)
- Safeguarding Vulnerable Groups Act (2009)
- Keeping Children safe in Education 2021

In addition to this, local procedures can be found at the Northamptonshire Children's Safeguarding Partnership website.

5. Aims

The aims of this policy are to:

- emphasise the need to educate staff, children and parents about the advantages and disadvantages of using new technologies within and outside the Schools.
- provide safeguards and rules for acceptable use to guide all users in their online experiences.
- ensure adults are clear about procedures for misuse of any technologies both within and beyond the Schools, and how to manage breaches of policy in accordance with safer working practices.
- develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and the potential issues related to technologies.
- safeguard our children and educate staff and parents by promoting appropriate and acceptable use of information and communication technology (ICT).
- outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
- ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, homophobia, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We refer to these four areas of risk when planning our approach to online safety and ensuring that we are safeguarding children against a broad spectrum of potential online harms.

6. Acceptable Use - Protocol, procedures and sanctions

6.1 Adult Responsibilities

All adults (employees or volunteers) have a shared responsibility to ensure that our children are able to use the internet and related technologies appropriately and safely. All adults in the setting are bound to the terms and conditions outlined in this document and a copy of this document is made available to all staff and shared with any volunteers, visitors or contractors.

6.2 Specific Responsibilities

(I). Executive Head teacher and Governors: The Head and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head and Governors should:

- Designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is

addressed appropriately. All employees, students and volunteers should be made aware of who holds this post within the Schools.

- Ensure all staff and employees adhere to procedures and protocols outlined in the policies and guidance agreed by Governors.
- Provide a safe, secure and appropriately filtered internet connection for staff, children and families at nursery.
- Provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- Promote e-safety awareness across the seven areas of learning as set out in the Early Years Foundation Stage guidance (2012) and have an awareness of how this is being developed, linked with the Federation development plan.
- Ensure that any equipment which holds sensitive or confidential information and leaves the Schools is encrypted.
- Share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- Ensure that e-safety is embedded within all child protection training, guidance and practices.
- Elect an e-Safety Governor to challenge the Schools about e-Safety issues.
- Make employees aware of the NSCP Online Safety guidance.

(II). Online Safety Lead

The nominated Online Safety lead should:

- Recognise the importance of e-Safety and understand the Schools duty of care for the-Safety of all children and staff.
- Establish and maintain a safe ICT learning environment.
- Ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- With the support of the ICT provider, ensure that filtering is set to the correct level for all children and adults accessing the internet.
- Report issues of concern and update the Executive Head on a regular basis.
- Liaise with all members of staff so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.
- Co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.
- Maintain an e-Safety Incident Log (Appendix 1) to be shared with the Executive Head and Governors at governing body meetings.
- Implement a system of monitoring employee and children use of Schools.

(III). Individual Responsibilities

All staff, including volunteers and students under the age of 18, must:

- Take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- Ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- Report any e-Safety incident, concern or misuse of technology to the e-safety Lead or Head, including the unacceptable behaviour of other members of the Schools' community.
- Only use the Schools ICT systems and resources for all School related business and communications. Schools issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head, for example, for use in an emergency on an educational visit.
- Ensure that all electronic communication with children, parents, carers, employees and others is compatible with their professional role and in line with the Schools' protocols. Personal details, such as mobile number, social network details and personal e-mail should never be shared or used to communicate with children and their families.
- Not post online any text, image, sound or video which could upset or offend any member of the Schools communities or be incompatible with their professional role. The Governing Body requests that staff acknowledge and act on the fact that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- Protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.
- Understand that network activity and online communications on Schools equipment (both within and outside the School) may be monitored and should only be used for School business.
- Understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.
- Comply with current legislation.

Staff are asked to read and sign our Acceptable Usage/Use of digital technology rules (see Appendix 2).

(IV). ICT Technician

ICT Technician is responsible for ensuring that:

- the Schools ICT infrastructure is secure and not open to misuse or malicious attack.
- anti-virus software is installed and maintained on all school machines and portable devices.
- The Schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the e Safety Lead and the Designated Safeguarding Lead.
- any problems or faults relating to filtering are reported to Designated Safeguarding Lead and to the broadband provider immediately and recorded on the e Safety Incident Log (Appendix 1).
- users may only access the Schools network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- he/she keeps up to date with e -safety technical information in order to maintain the security of the school network and safeguard children and young people.
- the use of the Schools network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead via automatic e-mail to School Business Manager or Officer Manager.

(V). The Children

All staff recognise that it is important for children to be e-safe from an early age and that the nursery plays a vital role in this. The practitioners in the nursery support the children in using ICT as part of their learning experiences across all areas of the curriculum and believe that, used correctly, ICT will not only raise standards, but will also support practitioners in their work with children. Our internet access is designed expressly for our children and includes appropriate filtering to the age of our children. In line with our other policies that protect children from danger we provide as safe an internet environment as possible. All staff, therefore, must ensure that:

- Children use the internet and ICT technologies safely within the nursery under the direct supervision of a member of staff.
- Children's Internet access is planned to enhance activities that will support their learning.

- Children are helped to understand how to ask for help if they come across materials they may make them feel uncomfortable.
- Websites that are used during nursery sessions are checked prior to use and monitored.
- Login passwords are for the expressed use of the staff.
- Children begin to understand, and follow, the children's 'Acceptable Use Rules' (Appendix 2)

6.3 Inappropriate Use - Procedure for following up instances

(I). Staff - In the event of staff misuse, if an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head of Schools, who is the Designated Safeguarding Lead **immediately**. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- LADO (Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the e-Safety Incident Flowchart (Appendix1) for further details.

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

- Accepting or requesting children and their parents as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with children and their parents.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.
- Publishing defamatory and/or false materials about the Camrose Early Years Schools, children, colleagues or other partners on social networking sites.

(II). Children - In the event of inappropriate use by a child, an adult will immediately attempt to minimise or close the content and then take the necessary action.

6.4 Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff - Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

7. Reporting/Monitoring usage Procedures

7.1 Incident Reporting

In the event of misuse by staff or children, including use of the Schools networks in an illegal, unsuitable or abusive manner, a report must be made to the Head/Designated Safeguarding Lead immediately and the e –Safety Incident Flowchart and the Schools' safeguarding procedures will be followed (See appendix 1).

In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head, Network Manager and Senior Information Risk Owner (SIRO).

All incidents must be recorded on the E-Safety Incident Log (See Appendix 1) to allow for monitoring, auditing and identification of specific concerns or trends.

7.2 Monitoring ICT usage

The Schools' ICT technician will support the Executive Head, School Business Manager and E-safety lead to monitor and record user activity, including any personal use of the Schools ICT system (both within and outside of the Schools environment) and users are made aware of this in the Acceptable Use Policy.

8. AUP in practice: Procedures and Protocols

The Schools strives to embed e-Safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever possible when ICT is used. The principles and procedures outlined above are embedded into our Curriculum in the following ways:

8.1 The Curriculum

- Key online safeguarding messages are reinforced wherever ICT is used with staff and where appropriate in the learning experiences offered to our children.
- The Schools follows the Early Years Foundation Stage and the curriculum guidance for 'Technology' as outlined in the Development Matters Framework document.
- When using ICT if appropriate there are opportunities for informal discussions with the children about online risks and personal protection strategies.
- Parents and staff are signposted to national and local organisations for further support and advice relating to e -safety issues, such as Child line and CEOP (**C**hildhood **E**xploitation and **O**nline **P**rotection Schools)
- Staff will focus on the four C's when using ICT for education purposes with children; **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, homophobia, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism; **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes; **conduct of their colleagues:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

8.2 Use of email

- The Schools provides some staff with a professional email account to use for all Schools related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the

risk of allegations, malicious emails or inappropriate contact with children and their families.

- Staff members are advised not to engage in any personal communications (i.e. via Hotmail or Yahoo accounts) with current or former children/parents. If this should occur they should follow the rules outlined in the AUP and not publish defamatory and/or false materials about the Camrose Early Years Schools, children, colleagues or other partners.
- All emails should be professional in tone and checked carefully before sending, just as an official Schools letter would be.
- Staff should inform their line manager or the e-Safety Lead if they receive an offensive or inappropriate email via the Schools system.
- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the e-Safety Lead or Head.
- Account holders must never share their password with another user, or allow access to their email account without the express permission of the e-safety Lead or the Head.

8.3 Managing remote access

As technology continues to develop, schools and their staff are increasingly taking advantage of opportunities for off-site access and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Equipment such as laptops should always be packed, stored and secured when offsite e.g. not left in a car overnight.
- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption, passwords on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns) These should also be changed regular and good practice,

8.4 Internet Access and Age-Appropriate Filtering

	Camrose	**Parklands**	**Croyland**	**Highfield**
Broadband Provider	Schools Broadband	Schools Broadband	Schools Broadband	Schools Broadband
Service Provider	Talk Straight	Talk Straight	Talk Straight	Talk Straight
Filtering systems	Open Hive and Fortinet	Netsweeper	Netsweeper	Netsweeper
IT technician-company	EasiPC	EasiPC	EasiPC	EasiPC

Filtering levels are managed and monitored on behalf of the Schools which ensures that filtered access at the highest levels for all members of staff and children. In addition to the above, the following safeguards are also in place:

- Anti-virus and anti-spyware software is used on all network and standalone PCs of laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users.
- The expectations for the online conduct of staff is addressed above staff are required to preview any websites before use, including those which are recommended to, or by, parents

9. Use of Schools and Personal ICT equipment

A log of all ICT equipment (including serial numbers), is maintained by the Admin Teams.
With respect to the ICT equipment owned, or used by the Schools:

- Personal or sensitive data is not stored on Schools devices (e.g. laptops, iPads, PC or USB Memory Sticks) unless encryption software is in place. This is true also of any photographs or videos of children.
- All such material should be stored either on the Schools network or on an encrypted device and deleted when no longer required.

- Time locking screensavers are in place on all devices in Schools to prevent unauthorised access, particularly on devices which store personal or sensitive data.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the Schools network without explicit consent from the Network Manager and a thorough virus check.

9.1 Mobile/Smart Phones

Staff/Visitor use:

- All staff must ensure that their mobile phones, personal cameras and recording devices are stored securely in their lockers or drawers during working hours or when on outings (This includes visitors, volunteers and students).
- Mobile phones must only be used in the private offices and the staff room the Schools (unless authorised by the Head).
- During Schools outings nominated staff will have access to a Schools mobile/personal phone which can be used for emergency contact purposes.
- It is the responsibility of the adult to ensure that there is no illegal or inappropriate content stored on their device when brought onto Schools grounds.
- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos or photographs of the children. Schools issued devices **only** should be used in these situations.

9.2 Laptops/Hand-held devices (e.g. iPads/tablets)

- Staff must ensure that all sensitive Schools data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection alone is not sufficient.
- Staff are aware that all activities carried out on Schools devices and systems, both within and outside of the Schools environment, will be monitored in accordance with this policy.

10. Photographs and Videos

Digital photographs and videos are an important part of the learning experience for our children. We recognise our responsibility to ensure that our children learn about the safe and appropriate use of digital imagery, and that our staff model good practice. To this end, there are strict policies and procedures for staff, children and parents about the use of digital imagery within the Schools.

- Written consent will be obtained from parents or carers before photographs or videos of young people are taken or used within the Schools environment, including the Schools website or associated marketing material
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.
- Permission will be sought from any child or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Images will never show children in inappropriate clothing.
- Digitised images will be deleted from devices immediately after they have been used. Unused photographs will be destroyed (shredded) or returned directly to parents.
- Staff will ensure that parents/visitors do not use mobile phones or other hand-held devices in the Schools.
- Parents are requested not to use their mobile devices or any photographic equipment on Schools premises.

11. Parent/Carer Involvement

As part of the Schools commitment to developing e-Safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

- All parents/carers will be made aware of our 'Technology Rules' (see Appendix 2).
- E-Safety information will be provided to carers to help raise awareness of key internet safety issues and how to keep their children safe on the internet.

12. Use of Social Networking Sites

Staff and parents are advised against the misuse of network sites such as Facebook to share confidential or potentially negative or abusive comments regarding the Schools, a member of staff, parent or child. This is referenced in the Schools code of conduct.

Appendix 1

- E-safety incident log
- E-safety incident flow chart

Foundations for Children
Nursery Schools Federation

e-safety and misuse of technology incident log

All misuse of technology and online safety incidents must be recorded on the form below.
The e-safety Lead and or the Designated Lead for Safeguarding will be responsible for monitoring incidents regularly and reporting any concerns to the Governing Body or appropriate agencies.

Date/ Time	Name of child/practitioner/adult	Nature of incident intentional/ unintentional/unknown	Details of incident	Action taken by whom/when/why	Who has been informed and how has the incident been recorded

Foundations for Children
Nursery Schools Federation

Signed: Date:

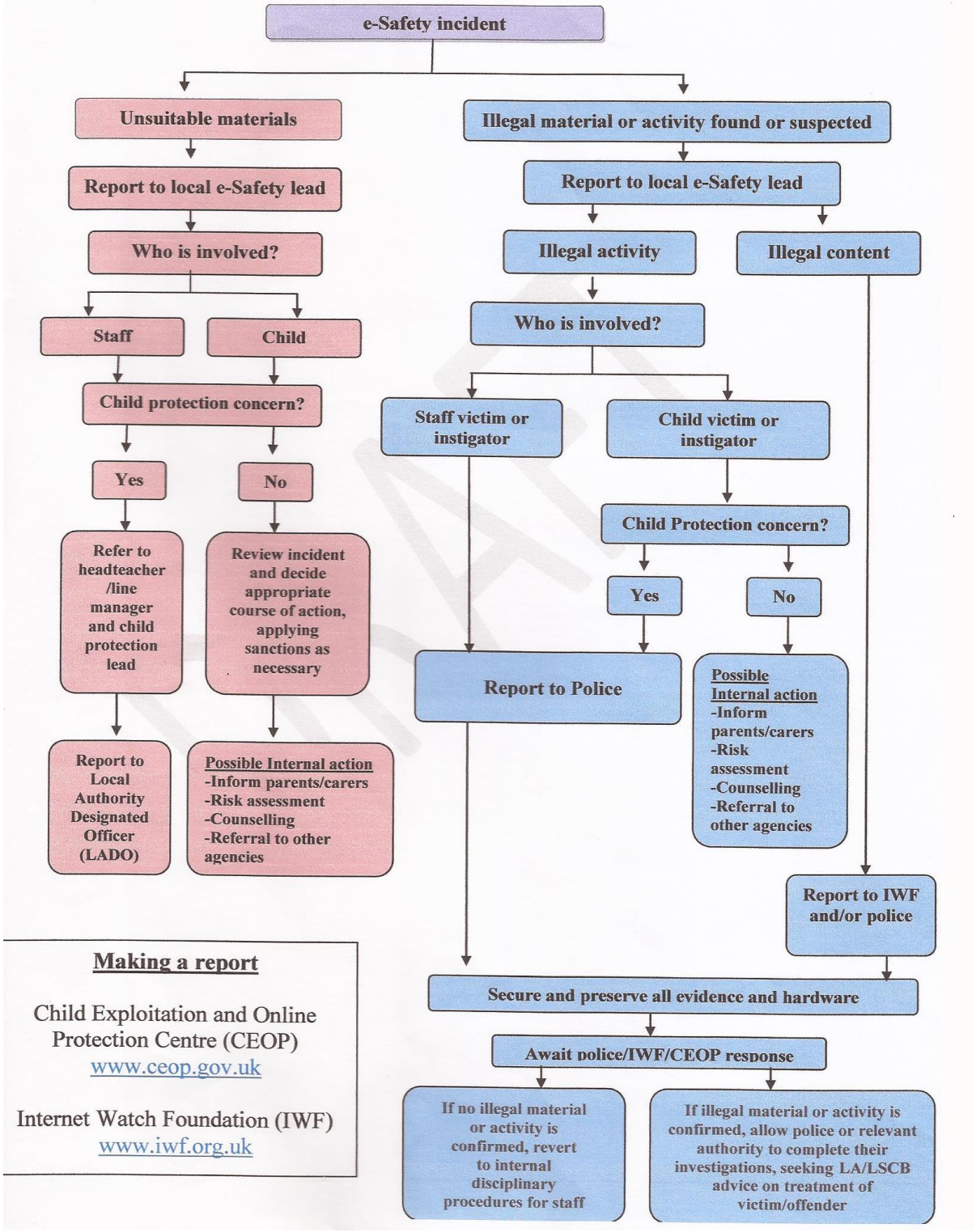
Executive Headteacher:

Chair of Governors:

Foundations for Children
Nursery Schools Federation

Croyland Nursery School and Day Nursery | Highfield Nursery School | Parklands Nursery School – Learning through play | Camrose

Northamptonshire LSCB e-Safety incident flowchart



Making a report

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.gov.uk

Internet Watch Foundation (IWF)
www.iwf.org.uk

Foundations for Children
Nursery Schools Federation

Appendix 2

- Acceptable usage and use of digital technology rules for staff and visitors
- Acceptable usage rules for children, parents and visitors

Foundations for Children
Nursery Schools Federation

To ensure that all adults within the Schools are aware of their responsibilities when using any on-line technologies, such as the internet or email, they are asked to sign these Acceptable Use Rules. Adults must provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform, protect and ensure that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Foundations for Children Nursery Schools Federation 'Acceptable Use Rules' for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded/accessed or printed.

- I have read and understand the Online/E-safety policy document
- I understand there are procedures/sanctions in place to ensure safe online practices
- I know that I should only use the school equipment in an appropriate manner and only for professional purposes.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the procedures for incidents of misuse so that I can deal effectively with any problems that may arise.
- I will report accidental misuse and any incidents of concern for children's or young people's safety to the Designated Safeguarding Lead or e-safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I will record/report incidents of cyber-bullying, reporting to the Designated Lead for Safeguarding or in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Lead and e-safety leads are.
- I know that I am putting myself at risk of misinterpretation or potential allegation should I contact children or parents via personal technologies, including my personal e-mail and should always use the Schools email and phones.
- I know that I should not be using the Schools' devices and system for personal use.
- I will only install hardware and software I have been given permission for.
- I will ensure that I use encrypted devices when transferring data or personal images
- I will ensure that I follow the Data Protection Act (1998) and have checked I know what this involves.
- I accept that the use of any technology designed to avoid or bypass Schools' filtering systems is forbidden.

Foundations for Children
Nursery Schools Federation

- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Lead.
- I have been given a copy of the Acceptable Use Policy in order to refer to e-Safety issues and produces that I should follow.
- I will adhere to copyright and intellectual property rights.
- I have received regular e-Safety information to highlight the risks to my own and the children's online safety.
- I know who to go to if I have any further questions.
- I am aware of the professional risks of using social networking sites and the Schools''s and Local Authority's perspectives on these. I know that if I use these sites I do so at my own risk as their usage is not condoned.

I have read, understood and agree with these rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies. I also understand that if I fail to comply with policies and protocols that I could be faced with disciplinary procedures.

Name (printed)……..

Signed……

Date……

Foundations for Children
Nursery Schools Federation

To ensure that our staff are fully aware of their responsibilities with respect to the use of digital images. They are asked to sign the following acceptable use agreement.

Foundations for Children Nursery Schools Federation Acceptable Use Agreement: Digital Images

Digital images refer to both still and moving digital photographs

- I have read and understand the Federation's use of ICT equipment sections in the e-Safety/Acceptable Use Policy document.
- I understand that all photographs taken of the children and families associated with the Schools and those taken outside on visits, are the property of the Schools.
- All digital images will be taken with Schools equipment. I understand that I may not use personal equipment to take images.
- Photographs will be stored on the Schools' computers for one academic year, unless taken specifically for marketing purposes and used for the School's website. After this time they will be deleted.
- I understand and agree that the Schools may monitor my technology use to ensure the safe use of digital images of the children and families associated with the Schools.
- I agree to comply with parental wishes in respect of the use of digital images of their children and families.
- I understand and agree that any photographs of children to be used in the Schools' promotional materials on the websites will not include names of the children.
- I agree to ensure that the pictures taken show respect, care and sensitivity towards the individual i.e. children will be dressed appropriately
- I understand that I am responsible for ensuring that the equipment assigned to / being used by me is fit for purpose and that such devices are secure/locked away when not being used.

I have read, understood and agree with these rules

Signed……
Date……

Name(printed)…….

School:…….

Foundations for Children
Nursery Schools Federation

E-Safety for Parents/Carers/Children

The safety and security of our children will always be one of our highest priorities. As such we would ask that you as parents /visitors support us by……

- Not using personal devices (e.g. cameras –pads/tablets etc.) in the Schools'.
- Being aware of the impact that misuse and inappropriate use of social networking sites such as Facebook and Twitter can have on our community.
- Having some knowledge of our Technology/ ICT policy and e-safety policy which can be found on our website or in our policies folder.

The children will have the opportunity to us ICT when they are at nursery and will be encouraged and supported to use it appropriately and safely by promising to…

- only use the internet when a grown-up is with them.
- use websites/apps that a grown up in Nursery or parent has chosen for them.
- ask a grown up for help
- be encouraged to walk away from the computer and find a grown up to help if they feel worried or unsafe.
- stay online by being encouraged to not talk about themselves when using the internet.

More details can be found in our e-safety policy and a copy of our Acceptable Usage Rules are on display in the Schools and online. You are welcome to have a copy of these so please ask a member of staff. Further information and advice can also be found at www.thinkuknow.co.uk

Foundations for Children
Nursery Schools Federation

Our Internet Rules

- We will only use the internet/apps together with a grown up.
- If we feel worried we will walk away from the computer and find a grown-up to help.
- We will try to stay safe by not talking about ourselves when we use the computer and find a grown up to help.
- We will try to stay safe by not talking about ourselves when we use the internet.
- We will always ask a grown up if we need help.

Updated in March 2023