Westfield Nursery School
Acceptable Use Policy

Date of document: 26/09/24
Date for next review: September 2025
Lead reviewers: E Collins/ P Heading

Changes: (in red)

- Added bullets to Other Staff and Children section
- Updated name of Designated Safeguarding Lead
- Added to School Owner Devices section
- Clarifies smart watches and sunglasses guidelines
- Added paragraph to Communication and Email section
- Added monitoring
- Added reporting misuse
- Added training

Vision
At Westfield Nursery we aim to deliver against our vision 'Inspired beginnings, outstanding futures'.

Rationale
To embed the safe use of ICT within the learning community and to enrich each child's learning opportunities and experiences in all curriculum areas & to fulfil the safeguarding requirements as set out in the Early Years Foundation Stage.

Aims
-To ensure the school's network is operated safely and all users of ICT are safe
-To ensure that all users are safe from bullying, crime and anti- social behaviour
-To enrich children's learning opportunities

Whilst our school promotes the use of technology or devices and understands the positive effects, they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the designated safeguarding lead in order for any necessary further action to be taken.

Roles and Responsibilities
This policy applies to all employees in the school, pupils, parents/carers, governors, visitors and outside agencies.

The use of ICT is monitored on a regular basis. Any person who is found to have mis-used the system or not followed this Acceptable Use Policy could face:

- withdrawal from the school system
- suspension or exclusion from the school
- disciplinary action
- in the most serious case legal action may be taken

The school's network and staff are organised to maintain the most secure environment possible

The Headteacher
The Headteacher takes ultimate responsibility for internet safety issues within the school, while delegating day to day responsibility to the online safety/ICT lead, and the whole staff team. The school will support online safety by:

- ensuring that the online safety lead is given time support and training to carry out their duties effectively
- ensuring that developments at local and partnership level are communicated to stakeholders
- develop an internet safety culture within the school
- ensure that the governing body is informed of the online safety issues within this policy
- ensuring that levels of funding support online safety
- promote internet safety to parents/carers

The Online Safety Lead
The online safety lead, Miss Heading will maintain a safe learning environment by:

- taking a lead role
- reviewing policy and procedure
- supporting the management protocols in an appropriate and consistent way, should online safety be breached

- attending appropriate training and development and ensuring the staff team and Governors are kept up to date with current trends
- helping to ensure staff are aware of their professional responsibilities for pupils' safety in this area
- maintain a log of incidents relating to internet safety in school

The Governing Body

The governing body at Westfield Nursery School has a statutory responsibility for Health and Safety and Safeguarding children and elements of this include internet safety. The appointed Safeguarding Governor, Miss Gee has specific responsibility for ICT and ensures that online safety is included as part of this.

The Governing Body will also fulfil their duty by:

- developing an awareness of ICT in school, particularly the internet and other communication technology devices
- ensure that they understand the school's policies, systems, and procedures for maintaining a safe ICT learning environment, by supporting the Headteacher in the implementation of these, including relevant training for all school staff
- support the Headteacher and the Strategic Leadership Team in developing a strategy to work with the media should a serious incident occur
- ensure the school budget meets the needs of the school's commitment to developing ICT in a safe learning environment

All Other Staff and Students

All members of the staff team have a responsibility to ensure that the teaching and learning environment is a safe place to be and to follow the protocols of this Acceptable Use Policy. They will do this by:

- maintain a professional level of internet access and use at home and at school in line with our Acceptable Use Policy (AUP)
- developing and maintaining knowledge of online safety issues, particularly about how it may affect young children
- plan classroom uses of the internet and ICT facilities to ensure that internet safety is not compromised, by, evaluating internet websites in advance of lessons and ensure that school filtering levels provide appropriate protection for topics being studied
- not attempting to bypass any filtering, monitoring and security systems
- not sharing school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so
- only using the internet for personal use during out-of-school hours, including lunch time
- only using recommended removable media and keep this securely stored.
- not searching for, viewing, downloading, uploading or transmitting any inappropriate material when using the internet

Guidelines

The Designated Safeguarding Lead (DSL), Miss Heading should be told immediately of any internet safety issue which would compromise the well- being of any child. It is the designated persons responsibility to seek training and development and act as a key member of the school's online safety team by:

- develop systems and procedures that support online safety in the school
- develop relationships with the local authority to provide advice and support in relation to Safeguarding, Child Protection and Internet Safety

Definitions

It is important to differentiate between inappropriate and illegal use of the internet. Procedures may also vary whether the access is deliberate or accidental. It is important to be clear about which type of incident has occurred.

Inappropriate Material
Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive such as:

- pornography
- hate material
- drug or bomb making recipes or related material
- sexist or racist material
- material used in any harassment
- material that others may find offensive
- defamatory, offensive, abusive, indecent or obscene materials
- material used in breach of confidence, privacy or trade secrets
- personal social networking using the school's Wi-Fi/hardware

Unlawful or Illegal Use
Unlawful or illegal use of the network includes accessing or having possession of material that contains:

- direct threats of physical harm
- child abuse images
- incitement to racial hatred or violence
- copyrighted, trademarked and other proprietary material used without proper authorisation

These are not exclusive categories and there may be other information that is deemed to be illegal.

Reporting Procedures
In all cases of incidents within school it may be necessary to review policies and procedures immediately after the event to prevent further cases occurring.

Procedures for Reporting Accidental Access to Inappropriate Material
Despite procedures in place, it is impossible to guarantee that there will never be accidental access to inappropriate or offensive material.

Anyone who accidentally comes across inappropriate or offensive material or pop ups must do the following:

1. Inform the online safety lead of the incident and give the website address or details of the email received
2. The online safety lead will log the web address or incident, time and username, in the web logbook, which is kept in the Head Teachers office
3. The online safety lead will inform the Headteacher (unless the Headteacher is directly involved in the incident)
4. The online safety lead will then make a judgement call on the severity of the incident and the effect it may have had on the pupils and may take further action such as informing parents, counselling the children etc.

Procedures for Reporting Suspected Deliberate Access to Inappropriate Material
Anyone who suspects another person of deliberately accessing inappropriate or offensive material must do the following:

1. Report in confidence to the online safety lead outlining reason for suspicion and details of the incident

2. The online safety lead will log the web address or incident, time and username in the web logbook which is kept in the Headteacher's office
3. The online safety lead will inform the Headteacher (unless the Headteacher is directly involved in the incident)
4. The Head Teacher will then report to the Local Authority Designated Officer (LADO)
5. If the investigation confirms that inappropriate behaviour has occurred, the Headteacher will follow school procedures and disciplinary proceedings may ensue on the grounds of misconduct or gross misconduct

Unlawful or Illegal Material
If you access any content including images, which you believe could be illegal, it is imperative that no attempt is made to investigate the content, and the incident is reported and logged immediately to the online safety lead. Do not print or take photos. Remove the device and give to the online safety lead immediately.

Procedures for Reporting Accidental Access to Illegal Material
Anyone who accesses the school network and who accidentally comes across illegal material should do the following:
1. Do not show anyone the content or make public the URL. If the content is an image in the body of an email under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence.
2. Report the incident to the online safety lead (children report to class leader who passes information onto the online safety lead)
3. The online safety lead will then log the web address or incident, time and username in the web logbook which is kept in the Head Teacher's office. This log reference is to protect you from any suspicion for having potential illegal material in your possession
4. The online safety lead will inform the Headteacher (unless the Headteacher is directly involved in the incident)
5. The Head teacher will then report to the LADO
6. Refer to the UK guidelines for sexting in schools and colleges guidelines if required https://www.gov.uk/government/publications/sexting-in-schools-and-colleges
NB- If a child takes a photograph of themselves this could be related to safeguarding/ child protection issues.

Procedures for Reporting Suspected Deliberate Access to Illegal Material
Any person suspecting another of deliberate misuse or abuse of the school network should take the following action:
1. Report in confidence to the online safety lead (or the Headteacher if the online safety lead is suspected) outlining reasons for suspicion and details of the incident
2. The online safety lead will then log the web address or incident, time and username in the web logbook. This can be found in the Headteacher's office. This log reference is to protect you from any suspicion for having potential illegal material in your possession
3. The online safety lead will inform the Headteacher (unless the Headteacher is directly involved in the incident)
4. If reporting a URL do not use copy and paste, type the URL
5. The Headteacher will then report to the LADO
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed, and criminal prosecution may follow

Mobile Devices

The term mobile devices refer to some of the following tablet computers, laptops, - USB portable memory devices, digital cameras, video cameras, mobile phones, SMART watches & SMART sunglasses. This is not an extensive list.

School Owned Devices

- Staff will only use school-owned devices for the purpose of carrying out school responsibilities. They will only access websites and apps that have been approved by the headteacher. They understand the usage of school-owned devices will be monitored.
- Images of the children and staff stored on any mobile device must be carefully monitored. Such mobile devices should be stored in a safe place. Any saved images must only be stored on password protected or encrypted devices. The saved images must also be stored in a safe place to prevent unauthorised access i.e. locked drawer, cupboard, safe or password protected mobile device. No images of the children should be taken without parental consent using any mobile device. See GDPR policy
- School-owned devices must be transported safely
- Parents/ carers must be contacted on school-owned devices using appropriate channels
- Damage or loss of my school-owned devices must be reported immediately to the Headteacher. Negligence may result in a cost to the individual
- School-owned devices must be returned to the school business manager upon the end of my employment at the school
- I will only install approved software onto school-owned devices
- School-owned devices will not be used to send inappropriate messages, images, videos or other content or to view, store, download or share any inappropriate, harmful or illegal content or to access personal social media accounts

Mobile Phones/ Smart Devices

- **Staff will ensure that personal mobile phones are locked away in their lockers.** Smart watches may be worn but must be disconnected from the internet and phone during the school day. Staff will be able to access their phones/ watches during scheduled breaks. If they are expecting an urgent call on their mobile, then it will be given to the office staff to keep and answer
- Smart sunglasses must not be worn during session times
- Visitors will be asked not to use mobile phones in the nursery. If for work purposes, visitors need to use their mobile phones they will be able to do so by leaving the nursery and using their phone outside or in a room away from the children
- There is no reason for a member of staff to have a mobile phone in the setting or on their person. If a member of staff is found to have a mobile phone on their person during the session this matter will be taken to the governors, it will be treated seriously with possible disciplinary action taking place
- Parents/carers will be made aware of this policy and posters will also be put in the nursery making sure that parents/carers/childminders do not use their mobile phones in the setting whilst dropping off or picking up their children. Any parent/ carer seen using their phone will be challenged by a staff member

Security of the Network

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

You are prohibited from storing, distributing, transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of any unlawful or illegal material through the network.

As a user of network, you agree not to use it to send or receive materials or data which is deemed inappropriate.

Passwords

The following rules must be followed regarding passwords to ensure the school is secure and monitoring can effectively take place.

- Each adult working within the school must access their accounts and any devices using their own passwords.
- Don't lose or give your password to anyone (if your password is lost or someone finds out what your password is inform the online safety lead)
- Always use your own secure password
- Always log off or lock the computer to prevent unauthorised access
- Use a complex password comprised of a minimum of 8 characters including lower and upper case letters, numbers and special characters or a pin number
- Never leave administration accounts logged on or unattended at any time

(See Cyber Security Policy)

Software and Downloads

- All users of the network must virus check any USB device storage devices before using on the network
- All USB devices must be encrypted, and password protected
- All users are prohibited from installing software onto the network from a CD-ROM or other device without permission from the ICT lead
- All users are prohibited from downloading software from the internet without permission from the ICT lead
- Copyright and intellectual property rights must be respected when downloading from the internet

Communication and Email

The school currently uses RM Education Services for internet connectivity and filtering. The school uses Microsoft Office 365 for digital communication.

Users are responsible for email they send and for contacts made and should be aware that these are open to be read and should be treated as public.
E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. When sending an e-mail using the school network the use of abusive language (swearing) is strictly forbidden. Make sure nothing in the messages could be interpreted as libellous. Racist comments must never be sent using e-mail or any racist e-mails forwarded using the school's network. Online bullying using e-mail will not be tolerated.

E-mail attachments should only be opened if the source is known and trusted. The opening of spam e-mails should be avoided as these often carry viruses that may damage the school network. Any e-mails that appear to be spam should be deleted rather than opening. Spam e-mails, promotional or advertising material and chain mails must never be sent or forwarded from any computer within school.

Staff should only use the approved email accounts that have been provided when sending communications regarding school business and ensure any personal

information that is being sent via email is only sent to the relevant people and is appropriately protected.

Staff will not use personal emails to send and/or receive school-related personal data or information, including sensitive information or use personal email accounts to contact pupils or parents.

E-mail addresses must never be broadcast publicly. Parents are to send emails to the office email office@westfieldnurseryschool.org or class emails
Bumblebees- bumblebees@westfieldnurseryschool.org
Dragonflies- dragonflies@westfieldnurseryschool.org
Ladybirds- ladybirds@westfieldnurseryschool.org
Caterpillars- caterpillars@westfieldnurseryschool.org
Butterflies- butterflies@westfieldnurseryschool.org

Uploading Images/Videos
All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable. Please see the school's photograph policy which is kept in the School Policy File. No photographs or videos which include nudity or inappropriate actions are permitted to be downloaded under any circumstance as this constitutes misuse.

Network Protocol
- School computer and internet use must be appropriate to a pupil's education or to staff professional activity
- Respect other people's material and do not corrupt, interfere with or destroy them. Do not open other people's files without express permission
- When working with RM Integris or any other personal data ensure that the data is secure

Internet Usage
Children **must** always be supervised when using the internet.
Activities should be planned so 'open searching' is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
When searching the internet with pupils 'child safe' search engines should be used such as: https://swiggle.org.uk/

The use of public chat rooms and messaging systems (e.g. ICQ, MSN Messenger) is not allowed on school machines. Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.

Social Networking
The school has a
Facebook account: Type Westfield Nursery into your search bar and scroll down until you find accounts rather than pages
Twitter account: WestfieldNews76
Instagram account: westfield_nursery

These are not currently being used. One member of staff is responsible for these accounts- Miss Dhenin (Deputy DSL). She will monitor the accounts. You tube may be used for specific messages e.g. welcoming new children to the setting with the permission of the adults involved.

To ensure compliance the following should be noted:

- **Staff should not accept parents as friends on any social networking sites**. If a member of staff already has a parent on a social networking account (someone they know in the community), they should report this to the Headteacher who will keep a record
- There will be no mention of the nursery, names of staff, governors or attending children or their families
- All staff should bear in mind that information they share through social networking applications, even though they are on private spaces, are still subject to copyright, data protection and freedom of information legislation, the safeguarding vulnerable groups act 2006 and other legislation
- Staff can follow the Westfield accounts but should ensure that their own personal accounts have the highest privacy settings enabled
- Sites to be aware of include: Social networking sites (e.g. Facebook, Instagram), blogs (e.g. Blogger), discussion forums (e.g. Mums net), collaborative spaces (i.e. Wet paint), media sharing services (e.g. You Tube) and microblogging (i.e. Twitter)
- Photos of staff, children or their families on any site will only occur with written permission
- Any communications or content you publish that causes damage to the setting or any of its employees, children or families may amount to misconduct or gross misconduct and could lead to dismissal

Monitoring

The school may undertake monitoring activities of employees to ensure the quality and quantity of work. The school will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the school will ensure employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and it is as unintrusive as possible to the employees.

Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance. The school will conduct its monitoring activities in a way that's fair and reasonably expected, with transparency, clearly explaining how and why they process my information. The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR.

Reporting misuse

Staff will report any misuse and recognise the consequences of breaches of this policy

Possible Sanctions for Misuse

Any person who is found to have misused the school system or not followed the schools Acceptable Use Policy could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken

Training

Staff will act as role models. They will take part in training and cyber security updates as required.

Policy Review
This policy will be reviewed annually. The policy may also be reviewed in response to technological advances and in the event of the need to change procedures and practices within the policy.

For further information please refer to:
-Keeping children safe in education (KCSIE 2024)
https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf
-Children's exploitation online protection (CEOP) https://www.ceop.police.uk/safety-centre/
-UK Safer internet centre https://www.saferinternet.org.uk/about

Vision
At Westfield Nursery we aim to deliver against our vision ‘Inspired beginnings, outstanding futures’.

Philosophy
Westfield Nursery School has a commitment to keeping children safe and healthy and the online safety policy operates under the umbrella of the Safeguarding and Child Protection Policy. The online safety policy is the implementation of the Safeguarding policy in relation to electronic communications of all types and use of the internet.

Aims
1. That our duty to safeguard children is maintained
2. That the setting is not exposed to legal risk
3. That the reputation of the setting is not adversely affected
4. That our users can clearly distinguish where information provided via social networking applications is legitimately representative of the setting
5. That we do not damage our reputation
6. That we recognise our legal responsibilities

Guidelines
The Internet is now regarded as an essential resource to support teaching and learning. Computer skills are vital to accessing life-long learning and employment.

It is important for children to learn to be e-safe from an early age and our nursery can play a vital part in starting this process.

In line with other nursery policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and a need to begin to teach them to be aware of and respond responsibly to possible risks.

Core Principles of Internet Safety
The Internet is as commonplace as the telephone or TV and its effective use is an essential life skill. Unmediated internet access brings with it the possibility of placing children in embarrassing, inappropriate and even dangerous situations.

As the internet is an essential element in life for education, business and social interaction, the nursery has a duty to provide children with quality internet access as part of their learning experience.

Nursery internet access will be tailored expressly for educational use and will include appropriate filtering. Pupils will learn appropriate internet use. Staff will guide pupils in online activities that will support their learning journeys.

The internet is also used in the nursery to support the professional work of staff, to allow effective planning and to enhance the nursery’s management information and business administration systems.

Guided Educational Use

Significant educational benefits should result from internet use including access to information from around the world. Internet use should be carefully planned and targeted within a regulated and managed environment

Risk Assessment
We have a duty to ensure that children in the nursery are not exposed to inappropriate information or materials. We also need to ensure that children know how to ask for help if they come across material that makes them feel uncomfortable.

Responsibility
Internet safety in the nursery depends on staff, parents, carers and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones. It is the nursery's responsibility to use technical solutions to limit internet access and to monitor their effectiveness.

Roles and Responsibilities
-The ICT Lead will ensure that the appropriate filters are applied to the PCs, laptops and iPads in the nursery and to the PCs/laptops in the office
-Staff will monitor the websites being used by the children during nursery sessions
-Staff may use the internet during sessions in order to view additional websites with the children, for example to look at sites related to themes they have been discussing
-Staff must ensure they exit immediately after viewing the sites to restrict access for the remainder of the nursery session
-If a member of staff uses the nursery PCs for schoolwork, again they must ensure they exit immediately on completing the work to ensure access is restricted for the remainder of or the next nursery session
-If staff or pupils discover unsuitable sites have been accessed on the nursery PCs etc., they must be reported to the Headteacher/ICT Lead immediately so that the filters can be reviewed
-Staff are responsible for ensuring that material accessed by children is appropriate and for ensuring that the use of any internet derived materials by staff or by children complies with copyright law
-The point of contact on the website should be the Nursery address, nursery email and telephone number. Staff or children's home information will not be published.
-Website photographs that include children will be selected carefully and will not allow individual children to be clearly identified. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers for featuring their child on the website is requested when each child starts at the nursery and parents/carers wishes are always followed

Harmful Online Challenges and Hoaxes
A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

If staff become aware of such challenges/ hoaxes they should inform the DSL.

- The DSL should check the factual bases of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline (Professionals Online Safety Helpline | UK Safer Internet Centre) from the UK Safer Internet Centre.

- where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful.

Staff should avoid sharing upsetting or scary content to show children and young people what they “might” see online.

Communication
Managing email: Children will not have access to email. Staff using email will use a nursery email address. This address must not be used for personal email.

Parents and Online safety
Parents’ attention will be drawn to the importance of online safety through information provided in newsletters and on the website. We also promote online safety through safer internet day.

Handling Complaints
Any complaints about the appropriate use of the internet or other technologies will be handled through the Complaints procedure.

Westfield Nursery School
Social Networking Policy

Vision
At Westfield Nursery we aim to deliver against our vision 'Inspired beginnings, outstanding futures'.

Introduction
This policy provides the acceptable standards for the use of social networking for all school employees at Westfield Nursery School. It applies to all school employees, including casual workers.

This policy covers the use of social networking sites and applications, such as, but not limited to; Twitter, Facebook, You Tube, Snapchat, Instagram etc. It further includes blogging, online discussion groups or social networking groups.

Purpose
The purpose of this policy is to:

- Set out clear guidance of the acceptable use of social networking sites
- Ensure confidentiality of the school, staff and pupils is maintained
- Ensure that all school employees understand the consequences of failing to comply with the Social Networking Policy
- Ensure the appropriate use of the school's resources

First read the Social Networking Paragraph in the Acceptable Use Policy

Governing Body/Headteacher Responsibilities
It is the responsibility of the Headteacher to publicise and make this policy available to all current and future school employees, and to ensure that the standards within it are both monitored and enforced and to advise the governing body of any serious breaches of this policy.

It is the responsibility of both the governing body and the Headteacher to take corrective and disciplinary measures as are necessary when a breach of this standard occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards may constitute a criminal act.

Employee's Responsibilities
It is the responsibility of the school employee to read and comply with the Social Networking Policy. School employees are reminded that they are bound by the School's Code of Conduct and teaching staff are further subject to the teaching standards. Any concerns will be reported and dealt with via the school's disciplinary procedures.

All school employees are reminded that:

Everything posted online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed. Therefore, assume that everything that is written is permanent and can be shared.

School employees are reminded that they should:

- Have the highest standards of personal conduct (inside and outside of School)

- Ensure that their behaviour (inside and outside of school) does not compromise their position within the school
- Ensure that their judgment and integrity should not be able to be brought into question and that of the school

Any failure to abide by the Social Networking Policy will result in disciplinary action.

School employees must alert the governing body and/or Headteacher where a breach of these standards is suspected or known to have occurred. Failure to do so may result in disciplinary action.

Safeguarding Children

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. Employees must abide by agreed method of communication policies within school. Adults should ensure that all communications are transparent and open to scrutiny.

Safeguarding children is the responsibility of all school employees. The key principles are:

- School employees **must not** communicate, (including accepting 'friend' requests) with any current pupils of the school on social networking sites such as Facebook. This is applicable **even** if a school employee has permission from a pupil's parent/guardian. (This would not apply to current pupils that an individual employee is directly related to, e.g. their child, niece or nephew). School employees should not communicate with, including being 'friends' with past pupils whilst they are below the age of nineteen.
- The principles apply regardless of whether access occurs during or outside of contracted work hours.
- The principles apply to all technology whether provided by the school or owned by the employee.

Unacceptable Use of Social Networking Sites/Applications

Through Social Networking Sites/Applications, school employees **must not**:

- Disclose private and confidential information relating to pupils, parents, other school employees, their employment directly or the school
- Discuss or reveal any matters relating to the school, school employees, pupils or parents
- Identify themselves as a representative of the school
- Write abusive comments regarding school employees, pupils or parents/carers
- Harass or bully school employees, persons unrelated or related to the school through cyber bullying and social exclusion
- View or update their personal site (on Facebook, twitter etc) during the working day, unless on a designated break.
- By-proxy update their personal site (Facebook, twitter etc) during their normal working day, and must ensure that their social networking site/application is secure from third parties
- Access or share illegal material
- Publish any content, which may be deemed as defamation or discrimination
- Post any images of pupils
- Request permission from school employees before posting any images of them on a social networking site
- Set up and/or use an alias social networking account to circumvent the policy
- Breach any of the school's other policies and procedures such as the School's Code of Conduct or the Equal Opportunities Policy

- Use it as a forum for raising and escalating concerns regarding the school or the Council. These concerns should be raised using the Whistle Blowing Procedure

Westfield Nursery School
Photographs of Children Policy

Vision
At Westfield Nursery we aim to deliver against our vision 'Inspired beginnings, outstanding futures'.

Rationale
To provide guidance on the appropriate use of images of children developed with the use of digital and all electronic recording devices used at or on behalf of Westfield Nursery School.

Aims
To ensure that staff, parents, carers and all interested visitors at Westfield Nursery School make full and proper use of photographic images whilst meeting the law and preserving safety of children.

Guidelines
The guidelines focus on issues around rights of privacy, child protection and copyright ownership.

Typical Uses of Photographs
- Displays in the establishment of children's activities
- Learning journey folders
- Publications by Westfield Nursery School
- Westfield Nursery School website and social media accounts
- Performing arts including dance and movement, concerts
- Media including newspapers and television especially when some editors require children's names when publishing photographs

Governing Body
The governing body will formally adopt these guidelines as policy and good practice. The safeguarding governor will be made aware of and help to ensure the support of these policies and procedures.

Ownership
Human Rights legislation and GDPR legislation give people rights, and it is the right to 'privacy' that is the issue when using photographs. The school respects the rights of people in photographs.

The Copyright, Designs and Patent Acts 1988 moved the ownership of copyright to the photographer (or their employer) and away from the person commissioning and paying for the photographs, unless there is an agreement otherwise.

Guidelines
- The school will obtain the consent of the person in the picture or from their parent/ carer
- The school will have a signed agreement for photographs to be taken to be used in school
- The school will ensure that the image is used in its intended context only

If any photographs are used by the local or national press the staff will:
- *not name the child without the parent's consent*
- *not use the photograph out of context for any reason*

- *not use the photograph to illustrate sensitive or negative issues*
- *not publish or have the photograph published on any of the social media sites*

When Photographing Children, Adults at Westfield Nursery School will Ensure:

- Parents and carers have signed their consent on the new starter form or social media form
- Ensure all children are appropriately dressed
- Avoid images that only show a single child with no surrounding context of what they are learning or doing
- Not use images of a child who is considered very vulnerable, unless parents/ carers have given specific written permission
- Use photographs that represent the diversity of the young people participating
- Report any concerns relating to any inappropriate or intrusive photography to the Headteacher
- Remember the duty of care and challenge any inappropriate behaviour or language
- Do not use images that are likely to cause distress, upset or embarrassment
- Regularly review stored images and delete unwanted material- See GDPR policy

Parental Permission

- Use of images of children requires the consent of the parent/ carer
- When a parent does not agree to their child being photographed, the class teacher will inform staff and make every effort to comply sensitively
- When photographic images are transmitted or shared beyond the establishment e.g. television broadcasts, images on internet sites, specific permission will be obtained from the parents/carers of the individual children involved

Displays in Schools

Still photographs shown on displays and video clips available during 'open' days/ parents' consultations will depict children in an appropriate way.

Parents Consultations, Concerts, Presentations

To allow the appropriate recording of children's images by parents/ carers:

- ensure that children are appropriately dressed
- obtain parental permission
- be aware of any child who should not be photographed
- that still images only can be recorded, and the staff team will monitor the use of cameras/mobile phones and anyone behaving inappropriately.

Children Photographing Each Other

From time-to-time children will take photographs of each other these will be reproduced following the guidelines as stated above and deleted in a timely fashion

Newspapers

Photo opportunities:

- The teacher/Headteacher will seek to gain parental permission before the photographs are taken and will be sought for names to be published
- If this is not possible – for instance because a specific group of children have achieved something, and parental permission regarding the publication of full names is withheld for one or more of the group – the Headteacher will negotiate a 'first names only' agreement with the newspaper

Photographs taken at Westfield Nursery school either by staff or parents/ carers will not be posted on any social media site

Storage and Disposal
Images are to be stored and disposed of securely. The aim will be to prevent unauthorised access, ensure confidentiality and protect identity
Images will not be kept for longer than is to be considered necessary and no longer than a child's time at the Nursery. The Headteacher/GDPR Lead is to ensure all photographs are to be permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

Security
All images are to be handled as personal data and deemed to be of a sensitive and confidential nature. It is to be recognised that damage or distress could be caused if security is to be breached. The responsibility of being in a position of trust in handling such data must therefore be taken seriously.