Online-Safety and ICT Acceptable Use Policy

This policy is reviewed annually by the Governing Body and was last reviewed on 19th January 2015 and amended January 2017 and June 2020.

Signature **(Governor Representative)**

Print Name Lesley Pollard **Date**

Signature **(Headteacher)**

Print Name Julia Mann **Date:**

Signature **(e-Safety Lead)**

Print Name Kerry Wright **Date:**

Signature **(Designated Safeguarding Lead)**

Print Name Julia Mann **Date:**

Contents

Gloucester Nursery School

Online/e-Safety and ICT Acceptable Use Policy

1. Introduction

ICT and the Internet have become an integral part of our modern lives and an equally important feature of the educational landscape. ICT promises to provide our children, staff and parents with opportunities to improve understanding, access online resources and communicate with the world at the touch of a button. 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;
- E-mail, instant messaging, chat rooms and chat forums.

As a consequence of their age, the majority of the children at our Nursery school are unlikely to have been introduced to most of these applications/services. However, some may already be using them individually, whilst others will almost certainly have experienced parents/carers or older siblings using them. As such, 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 safe use of online technologies, both within the school and home environment. Our children will be helped 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 other users.

As some of the technologies listed above will be utilised by our own school community, 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[1] procedures must be clear, agreed and followed by everyone.

2. Why do we have an Acceptable Use Policy (AUP)/e-Safety/Online Safety[2] Policy?

The use of the Internet as a tool to develop learning and understanding has become an integral part of the Nursery and home life. There are always going to be risks to using any form of communication that lies within the public domain, and it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst 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 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 likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to our 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 clearly sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard the children and adults within our nursery community. The policy recognises the ever-

---

[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 'online safety' is taken to mean the safe and appropriate use of all web, mobile or network-based information, communication and storage technologies. The aim, through online safety, should be to reasonably protect all users of such technologies from potential harm or risk, through management of behaviour. The term 'e-safety' refers to the safe use of all electronic technologies, which may or may not be used with the internet, in order to protect users (children and adults) from potential and known risks.*

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 school to ensure the online/e-Safety of pupils when using the internet and other related technologies;
- The school's expectations for the behaviour of the whole school community whilst using the internet and related technologies within, and beyond, school;
- The school's expectations for the behaviour of staff when using ICT both professionally and socially as well as for accessing and using data.

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 that are brought onto school grounds. This policy is also applicable where staff, or individuals, have been provided with school issued devices for use off-site, such as a school laptop or mobile phone.

All schools are expected to ensure that non-employee's onsite are made aware of the expectation that technologies and the internet are used safely and appropriately. At Gloucester Nursery School, our Reception staff (or the person signing a visitor into the school) will be responsible for ensuring that this happens.

3.1 This document comprises Gloucester Nursery School's Acceptable Use Policy, Internet Policy, Camera and Digital Images Policy, Mobile Phone and Technologies 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;
- Staff Code of Conduct;
- Health and Safety Policy;
- Technology and ICT Policy;
- Whistleblowing Policy;
- Social Networking Policy (Appendix 3);

- British Values and the Prevention of Radicalisation and Extremism Policy.
- Data Protection Policy and privacy notices
- Complaints procedure
- Technology and Information Communication Technology

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 all school employees in relation to the use of technologies feature within the following legislative documents, which should be referred to for further information:

- The Children Act (2004);
- School Staffing (England) Regulations (2009);
- Working Together to Safeguard Children (2015);
- Education Act (2002);
- Safeguarding Vulnerable Groups Act (2009);
- Keeping Children Safe in Education (2016).

In addition to this, local procedures can be found at the NSCB website

5. Aims

The aims of this policy can be summarised as follows:

- To emphasise the need to educate staff, children and parents about the advantages and disadvantages of using new technologies both within, and outside of, the school environment;
- To provide safeguards and rules for acceptable use to guide all users in their online experiences;
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting, and how to manage breaches of policy in accordance with safer working practices;
- To 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;
- To safeguard our children and educate staff and parents by promoting appropriate and acceptable use of information and communication technology(ICT);

- To outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems;
- To ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that maybe applied.

All safeguarding responsibilities of schools and individuals referred to within the following AUP Policy includes but is not restricted to the legislation listed above

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 as part of the wider duty of care to which all who work in schools are bound. 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). Headteacher/Governors- The Headteacher and Governors have overall responsibility for Online/e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Headteacher and Governors should:

- Designate an Online/e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring online/e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school;
- 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 within the Nursery;
- Provide resources and time for the Online/e-Safety lead and employees to be trained and update protocols as appropriate;
- Promote Online/e-Safety awareness across the seven areas of learning as set out in the Early Years Foundation Stage guidance and have an awareness of how this is being developed, linked with the School Development Plan;

- Ensure that any equipment, which holds sensitive or confidential information and leaves school premises, (e.g. iPads, staff laptops and memory sticks) is fully encrypted;
- Share any Online/e-Safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to safeguarding and child protection;
- Ensure that Online/e-Safety is embedded within all safeguarding training, guidance and practices;
- Elect an Online/ e-Safety Governor to challenge the school about Online/e-Safety issues;
- Make all employees aware of the Northamptonshire Safeguarding Children's Partnership (NSCP) Inter-agency Child Protection procedures by going to www.northamptonshirescb.org.uk

(II). Online-Safety Lead

The nominated Online/e-Safety lead should:

- Recognise the importance of Online/e-Safety and understand the school's duty of care for the safety of all children and staff at the Nursery;
- Establish and maintain a safe ICT learning environment within the school;
- 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 in Nursery;
- Report, and record, issues of concern and update the Headteacher on a regular basis;
- Liaise with all members of staff so that procedures are updated and communicated, and take into account any emerging Online/e-Safety issues and technological changes;
- Co-ordinate and deliver employee training according to new and emerging technologies so that the correct Online/e-Safety information is being delivered;
- Maintain an Online/e-Safety Incident Log (Appendix 1), to be shared with the Head teacher and Governors at governing body meetings;
- Implement a system of regular monitoring of employee and pupil use of school issued technologies and the internet and record and action as required.

(III). Individual Responsibilities

All school-based employees, including volunteers and students under the age of 18, must:

- Maintain an understanding of this policy;
- Implementing this policy consistently;
- Take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly;
- Ensure that children 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 Online/e-Safety incident;
- Report, and record, any Online/e-Safety incident, concern or misuse of technology to the Online/e-Safety lead or Headteacher, including the unacceptable behaviour of other members of the school community;
- Only use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School 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 Headteacher (for example, for use in an emergency on an educational visit);
- Ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal email should not be shared or used to communicate with pupils and their families;
- Not post online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand 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 school equipment (both within and outside of the school environment) are monitored, including any personal use of the school network;
- 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

The ICT Technician is responsible for ensuring:

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

(V). The Children

The children are responsible for:

- Using the internet and ICT technologies safely within the school under the direct supervision of a member of staff;
- Informing adults of anything they find upsetting/inappropriate;
- Being supported to understand, and follow, the children's 'Acceptable Use Rules' (Appendix 2b).

(VI) Parents

- Notify a member of staff/Headteacher of any concerns or queries regarding this policy.
- Ensure parents have read, understood and agreed to the terms of acceptable use of the school's ICT.

(VII) Educating parents about online safety

- The nursery school will raise parent's awareness of internet safety in letters or other communications sent home and in information via our website. (Appendix 5)
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher or Deputy Designated Safeguarding Lead.
- Concerns or queries about this policy can be raised with members of staff or the Headteacher.

(VIII) Acceptable use of the internet in school

- All parents, staff, volunteers and governors are expected to sign an agreement regarding acceptable use of the school's ICT systems and internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by children, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

(IX) Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once through the academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- The DSL (and Deputy DSL) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy. (Appendix 6)

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 Headteacher **immediately**. The appropriate procedures for allegations must be followed (other policies may need referring to) and the following teams/authorities contacted:

- The Designated Officer at the Local Authority;
- The Schools' Senior HR Advisory Team;
- Police/CEOP (if appropriate).

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

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

Examples of inappropriate use
Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

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 Gloucester Nursery School, children, colleagues or other partners on social networking sites.

Using the internet to pursue radicalised or extremist views.

(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.

(iii). Parent - If a parent is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, safeguarding procedures will be followed and if necessary reference will be made to protocol outlined in the *Prevention of Radicalisation and Extremism Policy.*

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 school network in an illegal, unsuitable or abusive manner, a report must be made to the Headteacher immediately and the Online/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 Headteacher, Plumsun Data Controller and Senior Information Risk Owner (SIRO).

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

7.2 Monitoring ICT usage/Online Safety

As part of the "*Keeping Children Safe in Education 2016"*[3], updated statutory guidance for schools was provided by the DfE. This document states that:

> *"The school [must] ensure that there is not only appropriate filtering in place, but that the school is proactive in monitoring internet usage (pupil and staff). Governing Bodies are reminded to avoid internet filters that might "over block" therefore placing unreasonable restrictions on what children can be taught. The focus must be on an effective Online Safety (formerly known as e-Safety) curriculum to teach about managing risk."*

The Nursery School's ICT technician will support the Headteacher, Office Manager and Online/e-safety lead to monitor and record user activity, including any personal use of the school ICT system (both within and outside of the school environment) and users are to be made aware of this in the Nursery's Acceptable Use Policy (AUP). User activity will be reported to Governors at each full governing body meeting as part of the "Safeguarding" report.

8 Online Safety

8.1 AUP in practice: Procedures and Protocols

The school strives to embed Online/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**:**

8.2 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 school follows the Early Years Foundation Stage and the curriculum guidance for 'Technology' as outlined in the Development Matters Framework document. We also follow our Technology and ICT policy.
- When using ICT if appropriate there are opportunities for informal discussions with the children about online risks and personal protection strategies.

[3] Revised 2016, and available at - https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

- Parents and staff are signposted to national and local organisations for further support and advice relating to Online/e -Safety issues, such as Childline and CEOP (**C**hildhood **E**xploitation and **O**nline **P**rotection centre)

8.3 Use of email

- The school provides some staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows 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 must not engage in any personal communications (i.e. via Hotmail or Yahoo! accounts) with parents and must not communicate with current or former pupils until they have left education. If this should occur, it must be reported to the Headteacher.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- The school uses the online programme 'Tapestry' to send emails to parents about their child's learning. Some of these emails contain photographic images. All parental email addresses are used for school use only and securely locked away. Email addresses are used solely for this programme. Staff only use secure accounts, which are to be used with this package only as a means of facilitating a dialogue with the parents. When information is no longer needed, it is deleted.
- Staff should inform their line manager or the Online/e -Safety Lead if they receive an offensive or inappropriate email via the school 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 Online/e Safety Lead or Headteacher.
- Account holders must never share their password with another user, or allow access to their email account without the express permission of the Headteacher.

8.4 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. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in

any way that would violate the school's terms of acceptable use. 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);
- Passwords should not be shared with others
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be. They should only be sent via the schools system.

8.5 Internet Access and Age-Appropriate Filtering

Broadband Provider: EMPSN (Capita)

Service Provider:

Our children may have opportunities to access supervised safe and secure internet usage as part of the learning experience. The Headteacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored on behalf of the school by RM Safety net plus which ensures that filtered access at the highest levels for all members of staff and children. For changes to filtering levels, staff need to contact RM Safety net plus directly.

  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;
- Encryption codes on wireless systems prevent hacking;
- Parents are made aware of the CEOP Report Abuse button on leaflets, posters displayed in the Nursery as well as on the nursery's

website. Staff are reminded of this on displays and via training. Therefore, parents and staff are empowered to report online safeguarding issues.

The expectations for the online conduct of staff is addressed above staff are required to preview any websites before use, including those that are recommended to, or by, parents.

9 Use of School and Personal ICT equipment

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

- Personal or sensitive data is not stored on school 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 school network or on an encrypted device and deleted when no longer required;
- Time locking screensavers are in place on all devices in school 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 school network without explicit consent from the Network Manager or ICT Co-ordinator 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 during working hours or when out on outings (This includes visitors, volunteers and students);
- Mobile phones must not be used in any teaching area in the school (unless authorised by the Headteacher) or within toilet or changing areas;
- During school outings nominated staff will have access to a school mobile/personal phone (if authorised by the Headteacher) 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 school 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. School 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 school 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.
- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Headteacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc.) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

9.3 Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. pupil attainment and assessment data) off site, only encrypted memory sticks will be used.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

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 any digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of children will be taken or used within the school environment, including the school website or associated marketing material (see Appendix 4)

- 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.
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Headteacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.
- Where photographs of children are published or displayed (e.g. on the school website) first names only will be displayed.
- Wherever possible, group shots of children will not be taken (unless for display purposes), and images should never show young people in compromising situations or 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 are to ensure that parents/visitors do not use mobile phones or other hand-held devices to take pictures of their children during nursery sessions.
- Parents and carers are permitted to take photographs of **their own** children during a school production or event. The school protocol requires that photos of other people's children are not published on social networking sites.

11 Parent /Carer Involvement

As part of the school's commitment to developing Online/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).
- Online/e-Safety information will be provided to carers to help raise awareness of key internet safety issues and highlight safeguarding measures in place within school.

12 Staff 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 school, a member of staff, parent or child. All staff have seen and follow the WNC document 'Use of social networking – a guide for professionals working with young people' (Appendix 3)

13 Policy Review

The Online/e-Safety and ICT Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure.

Policy written:

This policy has been agreed by Governors at Gloucester Nursery School on (date) ……

Signed……..

Review date……..