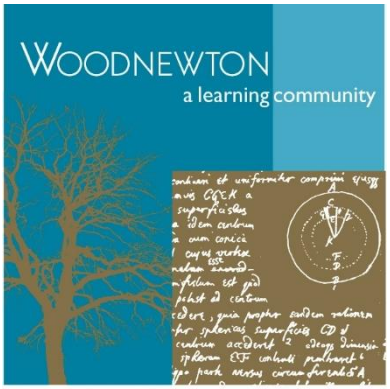
Woodnewton – a learning community

Online Safety Policy

Last Reviewed	**October 2022**
Next Review Due BY	**October 2024**



Inspiring Futures
Through Learning

Contents **Page**

1. Introduction

1.1 The aim of this policy is to set out key principles and expectations for all members of the School community with regard to the use of ICT-based technologies. The policy is designed to help safeguard and protect both children and staff in our School.

1.2 The relevant technologies to which the policy is applicable include, in addition to computers and associated hardware, all electronic devices such as mobile phones, games consoles, cameras and webcams.

1.3 In respect of interaction with children the DSL and SLT will assist staff to work safely and responsibly when utilising the internet and other communication technologies by supporting them in monitoring their own standards and practice.

1.4 There are clear structures in place both to minimise the risk of misplaced or malicious allegations made against staff who work with children and to deal with online abuse such as cyberbullying, sexting (sending and/or receiving personally intimate images) and identity theft including 'frape' (hacking facebook profiles). Guidance is given to all new staff about keeping themselves safe in our induction process.

1.5 Ofsted describes Online Safety (in relation to Schools and academies) as the ability to protect and educate children and staff in their use of technology at the same time having appropriate mechanisms in place to intervene and address any incident as and when necessary.

1.6 This policy will be communicated to staff and children (and the wider community) via School classrooms/staff rooms and website and will be an integral part of the School induction pack for new staff.

1.7 All members of staff in the School (and indeed the wider community) are encouraged to exercise vigilance and to be proactive in reporting issues, in the confidence that such concerns will be dealt with quickly and sensitively, through the School's escalation processes.

2. Purpose and scope

2.1 This policy is applicable to all members of our School community who have access to School ICT systems, both on and off School premises. This may include volunteers, parents/carers, visitors, and community users in addition to staff and children.

2.2 The following extract is taken from the DfE publication 'Preventing and tackling bullying: Advice for principals, staff and governing bodies - March 2014':

> *"The wider search powers included in the Education Act 2011 give teacher's stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones*."

2.3 The principle of protecting children includes the provision of a safe learning environment by use of appropriate monitoring and filtering to control what may legitimately be accessed by children whilst at the School. Essentially, however, this only protects them whilst they are on School premises. Ensuring provision of appropriate education relating to Online Safety is the only way to guarantee that, irrespective of their whereabouts, they know how to stay safe online.

2.4 The aim of this policy (and indeed of our School) is both to provide appropriate safeguards and to raise awareness to enable children (and others) to control their online experiences and thereby feel confident and secure in their use of technology. The entire School community needs to be fully aware of the risks (as well as the undoubted benefits) of information technology and accordingly must undertake to use it in a responsible manner.

2.5 Children will be instructed in the acceptable use of ICT at the School, and will be given clear and principled advice and guidance for general use of mobile technologies including the internet. Appropriate objectives are made clear and are displayed around the School, particularly where internet access is most frequent e.g. computer suites.

2.6 The Online Safety policy is integrated (and consistent) with other relevant policies. These include the following: Behaviour Policy; (Staff) Disciplinary Policy; Safe Working Practice Policy; Social Media Policy and the Child Protection and Safeguarding Policy.

3. Individual roles and responsibilities

3.1 Head

- To take overall responsibility for the provision of Online Safety
- To ensure the School uses an approved, filtered internet service, which is fully compliant with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles
- To ensure that robust systems are in place to monitor and support staff who carry out internal Online Safety procedures (e.g. network manager)

3.2 Online Safety Co-ordinator (Designated Safeguarding Lead)

- To have day to day responsibility for Online Safety issues and maintain a leading role in establishing and reviewing the School Online Safety policies
- To promote awareness and commitment to E-safeguarding throughout the School community
- To ensure that all staff are aware of procedures that need to be followed in the event of an Online Safety incident (including completion of an incident log)
- To regularly update their own knowledge and understanding of Online Safety issues and legislation (and to cascade this to other staff) and remain constantly aware of the potential for serious child protection issues
- To liaise with School ICT technical staff
- To liaise with the Local Authority and relevant agencies as appropriate

3.3 Governor

- To ensure that the School follows all authoritative Online Safety advice to protect the welfare of children and staff
- To approve the Online Safety Policy and regularly review the effectiveness of this policy
- To support the School in encouraging parents and the wider community to become engaged in Online Safety activities
- To undertake appropriate training and development on Online Safety issues

3.4 IT Manager

- To report promptly to the Online Safety coordinator any related issues that may arise
- To ensure that users may only access the School's network through an authorised password reinforced by a robust and properly enforced protection policy
- To ensure that provision exists for misuse detection and protection against malicious attack e.g. by keeping virus protection up to date
- To ensure the overall security of the School ICT system
- To ensure that access controls/encryption exist to protect all personal and/or sensitive information held on School-owned devices

3.5 Staff

- To read, understand and help promote the School's Online Safety policies and guidance by signing and adhering to the School's 'Staff Acceptable Use Policy' (Appendix 1)
- To be aware of Online Safety issues related to the use of mobile phones, cameras and other hand held devices and to monitor the use of such devices to ensure compliance with current School policies
- To report any suspected abuse or breach of policy to the Online Safety coordinator
- To maintain an awareness of current Online Safety issues, skills development and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their personal use of information technology

3.6 Children

- To understand the importance and seriousness of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Where appropriate have a good understanding (appropriate to their age and abilities) of research skills and the need to avoid plagiarism and uphold copyright regulations

3.7 Parents/Carers

- to support the School in promoting Online Safety
- to consult with the School if they have any concerns about their children's use of technology

4. Education, internet and the curriculum

4.1 The School provides repeated opportunities (within a broad range of curriculum areas) to learn about Online Safety and before using the internet children will be made aware of the relevant legislation such as data protection and intellectual property rights.

4.2 Children are also given advice if they experience problems whilst using the internet and are provided with guidance on promoting Online Safety including the requirements to:

- understand the importance of misuse (including accessing to inappropriate materials) and are aware of the consequences

- understand why they should not post (or share) detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure their privacy settings are appropriately configured
- understand why they must not post pictures or videos of others without their permission
- understand issues around plagiarism and how to check copyright etc
- know not to download any files – such as music files - without appropriate permission

4.3 The 'Children Acceptable Use Policy' (Appendix 2) reminds children about their responsibilities and details the strategies to maximise learning opportunities whilst reducing potential risks associated with use of the internet.

5. Managing the ICT infrastructure

5.1 In order to effectively manage internet access (including all relevant security issues) this School will:

- block all 'chat rooms' and social networking sites other than those which are part of a recognised educational network or approved Learning Platform
- only unblock (on a strictly temporary basis) other external social networking sites for specific purposes/internet literacy lessons
- ensure all staff have signed an acceptable use agreement form
- Inform all users that internet use is open to continuous monitoring
- make clear that in no circumstances is it acceptable for any individual to log on as another user
- set up the network with shared work areas for (separately) children and staff. Staff and children are given appropriate instruction in how to save (and subsequently access) work to (and from) these areas
- require all users to Lock screen at all times when they are leaving the computer unattended. If the user has finished with the computer, they must log off ready for the next user at all times. Where a user finds a computer which is logged on they are required to always log off and then log on again as themselves.

  In the interests of protecting themselves and others, children should bring such instances to the attention of a member of staff in order that suitable instruction may be offered to the previous user.
- set up the network so that users cannot download executable files/programmes
- make clear that the School's IT Manager is responsible for ensuring that all equipment that is taken off site has full anti-virus and spyware protection and that this is maintained up-to-date in accordance with School protocols and procedures
- make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the School is used solely to support their professional responsibilities
- ensure that access to the School's network resources from remote locations by staff is restricted to authorised personnel and that access is only through School approved systems

6. School website

6.1 The principal has overall responsibility for ensuring that the website content is accurate and that the quality of presentation is maintained and fully compliant with the statutory DfE guidelines for publications.

6.2 The content of the website will consist primarily of material created by the School itself. Where the content has been published by others (or there are links to such material) the sources will be credited, with a clear statement as to the author's identity or status.

6.3 Points of contact detailed on the website are likely to include the School postal address, telephone number and general email address. Home information or individual e-mail identities will not be disclosed.

6.4 Any photographs published on the web will not have full names attached to them and student names will not be used when saving images either in the file names or in the tags when publishing on the School website.

6.5 Teachers using School approved accounts (or similar) will be expected to ensure they are password protected and to run from the School website.

7. Use of ICT equipment at home

7.1 The School will (as and when resources permit):

- provide a laptop (or other IT equipment) for staff use at home or outside of School
- ensure that the equipment is working and that repairs are dealt with as quickly and effectively as possible
- ensure that the computer is covered by insurance for use in and out of School for study purposes, providing reasonable care is taken to prevent loss or damage
- ensure that the computer is protected against computer viruses and malware
- maintain and update any software used in School.

8. Use of digital and video photographic images

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have either recorded themselves or have downloaded from the internet.

8.2 However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may potentially cause significant harm or embarrassment to individuals in the short or longer term.

8.3 When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular children should be made aware of the risks attached to publishing their own images on the internet e.g. on social networking sites.

8.4 Images taken and used by the School will not be kept for longer than is necessary and will be subject to appropriate security measures.

8.5 Staff are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images:

- those images should only be taken on School equipment; the personal equipment of staff should not be used for such purposes
- care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute

- children must not take, use, share, publish or distribute images of others without their permission
- photographs taken by children for official School use will be controlled by the School
- photographs published on the website and other publications (e.g. newsletters etc.) that include children will be selected carefully and will comply with good practice guidance on the use of such images
- children' full names will not be used anywhere on a website or Tweets, particularly in association with photographs
- written permission from parents/carers (ie completion of the appropriate forms) will be obtained before photographs of children (or examples of their work) are published on the School website, around the School and in School publications.

9. CCTV and monitoring

9.1 The School has CCTV on the premises as part of site surveillance for staff and student safety. Recordings will not be revealed without permission except where disclosed to the police as part of a criminal investigation or where requests for disclosures can be considered under GDPR.

9.2 Specialist lesson recording equipment is used on occasions as a tool to share best teaching practice. These recordings are only accessible to authorised members of staff and will not be used for any other purposes.

10. Other policies and procedures

10.1 This policy will be supported by the following policies and procedures:

- Social Media Policy
- Child Protection and Safeguarding Policy
- Safe Working Practice
- Disciplinary Policy
- Behaviour Policy

Appendix 1

Staff Acceptable Use Policy: Online Safety

Principles

As an organisation with responsibility for safeguarding of children it is important that all staff take every possible necessary measure to protect data and information systems from unauthorised access, infection, damage, loss, abuse and theft.

All members of staff have a responsibility to use the School's information technology equipment in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and related School systems, they are asked to read and sign this Acceptable Use Policy.

Definitions

School Information and Communication Technology

This means any computer, networking device, telephone, copier, printer, fax machine, or other Information and Communication Technology equipment which

- is owned by the School or
- is licensed or leased by the School or
- is subject to School policies.

Roles and responsibilities

<u>The School</u>

The School owns the computers and the internal computer networks used on site. The School also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The School administers, protects, and monitors this aggregation of computers, software, and networks.

In its management of Information and Communication Technology, the School and its administrative department takes responsibility for:

- focusing central Information and Communication Technology resources on activities connected with teaching, learning and administration
- protecting School networks and other shared facilities from malicious or unauthorised use
- ensuring that central School computer systems do not lose important information because of hardware, software, or administrative failures or breakdowns
- managing computing resources so that members of the School community are not denied fair and equitable access to them
- establishing and supporting acceptable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of administrative information that the School maintains
- delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities

- monitoring policies and communicating changes in policy as events or technology may warrant
- enforcing policies by restricting access and initiating disciplinary proceedings as appropriate.

The Individual

The School supports networked information resources to further its mission of teaching and learning. All members of the School community must be aware of the rules and conventions that make these resources secure and efficient. Users of School Information and Communication Technology will take responsibility for:

- using resources efficiently, and accepting limitations or restrictions on computing resources - such as storage space, time limits, or amount of resources consumed - when asked to do so by systems administrators
- ensuring that programs from the internet are not downloaded or installed on any School computer: advice should be sought from the ICT Manager as appropriate
- protecting passwords and respecting security restrictions on all systems. If it is believed that a third party is aware of an individual's password the ICT Manager must be notified
- backing up files and other data regularly and permanently removing old files no longer required
- preventing unauthorised network access to or from their computers or computer accounts. This includes the responsible monitoring by staff of student users in their charge
- recognising the limitations to privacy afforded by electronic services
- respecting the rights of others to be free from harassment or intimidation
- honouring copyright, licencing and other intellectual property rights
- ensuring the physical protection of School Information and Communication Technology equipment. Any damage or theft shall be reported to the technical support staff immediately upon detection.
- ensuring responsible use of ICT equipment and ensuring children are following the Acceptable Use Policy
- reporting any faults, problems or requests to the ICT Support Team using the appropriate channels as soon as possible.

I understand that it is my responsibility to ensure that I remain up to date and read and understand the School's most recent Online Safety policies.

I have read and understood and agree to comply with the Staff Acceptable Use Policy: Online Safety

Signed: ……..... Print Name: …… Date: ……..…

Job Title: ……..

Appendix 2

Child Acceptable Use Policy – Online Safety

This Acceptable Use Policy is intended to ensure that young people will be responsible users while using the internet and other communications technologies for educational, personal and recreational use. The School will ensure that ICT systems and users are protected from accidental or deliberate misuse that could place the security of the systems and users at risk.

School strategy

The School employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a staff member
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material
- The School will regularly monitor children' internet usage
- Children and teachers will be provided with training in the area of Internet safety
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in School requires a teacher's permission
- Children will treat others with respect at all times and will not undertake any actions that may bring the School into disrepute
- Children must not take, use, share, publish or distribute images of others without their permission
- Children will ensure that they log out of their computer equipment when leaving the IT room.

World Wide Web

- Children will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Children will report accidental accessing of inappropriate materials in accordance with School procedures
- Children experiencing any issues related to viruses or anti-virus software should inform the ICT Technician without delay
- Children will use the internet for educational purposes only
- Children will not copy information into assignments without express acknowledgement of the source material (plagiarism and copyright infringement)
- Children will never disclose or publicise personal information

- Downloading by children of materials or images not relevant to their studies is in direct breach of the School's acceptable use policy
- Children will be aware that any usage, including distributing or receiving information whether School-related or personal, may be monitored for unusual activity, security and/or network management reasons

Use of digital/video images

The use of digital/video images plays an increasingly important part in learning activities. Children and members of staff may use digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the School website and occasionally in the public media.

We will ensure that when such images are published children cannot be identified by the use of their names.

Internet use and access is considered an School resource and privilege. Therefore, if the School policy is not adhered to this privilege will be withdrawn and appropriate consequences will be put in place

School Website

- Children will be given the opportunity to publish projects, artwork or School work on the world wide web in accordance with clear policies and approval processes regarding the content that may be included in the School's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of children or staff
- Website using facilities such as guest books, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details
- The publication of student work will be co-ordinated by a teacher
- Children' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission
- The School will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual children will not be published on the School website without parental permission. Video clips may be password protected
- Images will not be taken of any student against their wishes
- Photographs taken by our children will be controlled by the School and staff will ensure that they are appropriately supervised in line with the School Online Safety policy
- Personal student information including home address and contact details will not be included in School web pages
- The School website will not publish the names of individuals in a photograph
- Children will continue to own the copyright on any work published.

Personal Devices

Children are not allowed to use their own devices in School for personal use. This includes such use as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera.

All of these activities will be deemed to be in direct breach of the School's acceptable use policy. Children who need a mobile phone for walking to the School independently hand over their devices each morning and they are stored in the classroom until home time.

Legislation

The School will provide information on the following legislation relating to use of the internet (with which teachers, children and parents may care to familiarise themselves):

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures

The School will inform children and parents of key support structures and organisations that deal with illegal material or harmful use of the internet.