Woodlands Primary School

Information Security Policy

Written by	Corinna Taylor
Ratified by Governors	May 2021
Date for Review	May 2024
Signed – Chair of Governors	
Signed – Headteacher	
Is this an internal or external policy?	External
Is this based on a model policy?	No

Information Security Policy

	Contents	Page
1	Responsibility	3
2	Introduction	4
2.1	Information Security	4
2.2	Scope	4
2.3	Purpose	5
2.4	Breaches of the Information Security Policy	5
3	Information Security Roles and Responsibilities	5
4	Information System Security	7
5	Monitoring the Information Security Policy	10
6	Review of the Information Security Policy	11
7	Information Security – General	11
8	Information Security and Business Continuity	19
9	GDPR	21
10	Further Reading	21
11	Declaration	21

The purpose of this Information Security Policy statement is to describe how security is implemented, to give guidance to our employees whose actions can affect the confidentiality and integrity of the business, its product and services, and, to illustrate the overall commitment to security issues within our school.

1. Responsibility

Article 5(f) of the General Data Protection Regulation (GDPR) states that it is the responsibility of Woodlands Primary School to ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 32 (1) of the GDPR – taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Woodlands Primary School (Data Controller) and the processor shall

- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (Article 32 (1)(b));

- and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Article 32 (1)(d))

Article 32 (2) of the GDPR – in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

It is the established policy of Woodlands Primary School to operate within the requirements of a documented Information Security Policy statement as a means to comply with all statutory, regulatory and contractual requirements, and, to protect the interests, property and information of the school, and of its pupils and employees, against threats or loss.

In pursuance of this policy its stated requirements have been implemented together with the specified requirements of the school's associated information security and computer system access management work instructions.

This Information Security Policy statement, which is not intended as a stand-alone document, is supported by detailed process operating procedures and policies to form a set of working documents, which define our school's security activities.

The Information Security Policy is maintained by audit and review, in order to provide effective assurance that all aspects of school, employee and pupil specified security requirements are being implemented.

The Headteacher is responsible for managing information security, and the Headteacher will also ensure that all employees are trained to understand, implement and maintain the security objectives set out in this Security Policy and as detailed in the school's security related policies.

We publish this policy statement in the knowledge that the security of our school and its employees and pupils, and our on-going good security reputation, depend upon the everyday security awareness and actions of all our employees, both on-site and off-site.

2. Introduction

2.1 Information Security

The availability of complete and accurate information is key to providing excellent services to the pupils, parents, staff and governors of Woodlands Primary School. A large amount of sensitive and personal information on individuals, both pupils and staff, is held by the school.

Woodlands Primary School has a number of responsibilities to protect its reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the **confidentiality**, **integrity**, **availability** and **accountability** of this information needs to be protected from harm in a way that is proportionate to the risks to the information. This Information Security Policy provides the overall framework to help everyone play his or her part in protecting pupil, staff and governor information.

This policy is supported by a comprehensive set of processes, procedures and guidelines.

2.2 Scope

The Information Security Policy applies to all users accessing any ICT systems (such as computers, hand held devices, or any information storing or processing devices) and information owned and/or operated by Woodlands Primary School. This policy applies **wherever** and **whenever** school information is processed and applies equally to **all users** including:

- Teachers, Governors, Teaching Assistants, Associate Staff and Office Staff
- Contractors, consultants, casual and temporary employees and volunteers
- Partners and suppliers

The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled by Woodlands Primary School, including information, which is:

- Spoken face to face, communicated by landline or by mobile telephone
- Written on paper or printed out from a computer system. This may include working both onsite or remotely
- Stored on school server and the cloud
- Stored in structured manual filing systems and on the school server
- Transmitted by electronic mail, over the Internet and via wireless technology
- Stored and processed via computers, computer networks or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablets and ipads.

- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

2.3 Purpose

The purpose of the Information Security Policy is:

- To protect the School's information and subsequently to protect the School's reputation
- To enable secure information sharing to deliver services
- To protect the School from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the School's employees
- NOT to constrain reasonable use of information in support of normal business activities of the School

This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

2.4 Breaches of the Information Security Policy

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action.

Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user and/or their employer.

In certain circumstances, the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the General Data Protection Regulation (GDPR) could result in a hefty fine being issued to the individual and the organisation. Please see **Woodlands Primary School Data Breach Reporting Procedures Policy** for information.

3. Information Security Roles and Responsibilities

3.1 All information users including all employees, contractors, consultants, volunteers, governors, partners and suppliers must:

1. **Comply with** this Information Security Policy, processes, procedures and guidelines at all times.
2. Comply with legal, statutory, regulatory and contractual obligations related to information at all times.
3. Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to **confidentiality**, **integrity** and **availability**.
4. Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.
5. Report immediately all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the School's information or information systems, following agreed incident management policies and processes.
6. Read and act on any communications and training about information security and ask for clarification if these are not understood.
7. Play an active role in protecting information in day-to-day work.

3.2 Governors and School Senior Leadership Team

1. Approve this high level Information Security Policy.
2. Actively promote effective and appropriate information security by the use of structured risk assessment in all future developments and by appropriate retrospective risk assessment of current processes and systems.
3. Implement and promote Information Security to all staff and governors within their service areas.
4. Ensure that employees understand and abide by the Information Security Policy and its associated policies, processes, procedures, guidelines and understand its impact.
5. Assign owners to all information in their area of responsibility.
6. Provide effective means by which all staff and governors can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.
7. Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
8. Provide written authorisation for access to information.
9. Ensure that communications regarding information security are cascaded effectively to all staff.
10. Ensure that information security is an integral part of all departmental processes.

3.3 Information owners

Data sets may have different owners and where several potential information owners exist, responsibility should be assigned to the manager whose group makes the greatest use of the data.

1. Use structured risk assessment to select security controls to protect their information.
2. Monitor to ensure security controls continue to be effective and that information is being handled correctly.

3. Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
4. Manage the residual risks to their information.
5. Prepare appropriate Business Continuity plans and contingency arrangements.

3.4 ICT Services

1. Be the custodian of electronic information in its care by implementing and administering technical security controls and by the Information Owners as a result of information security risk assessment.
2. Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
3. Assist Woodlands Primary School to ensure all software is licensed and remove unlicensed software.
4. Provide contingency arrangements for information systems.
5. Provide appropriate protection from malicious software.
6. Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
7. Monitor and investigate technical security breaches.
8. Provide technical support to enable compliance with this policy.

3.5 Information Security Team

1. Provide agreed information security policies, processes, procedures and guidelines to assist Woodlands Primary School in protecting information appropriately.
2. Provide training and consultancy in assessing information risk and selecting appropriate security controls.
3. Provide a library of materials demonstrating good practice to assist in structured information security risk assessment.
4. Promote awareness of information security throughout the school and assist in ensuring that information security is an integral part of all departmental processes.
5. Liaise with information security specialists in other organisations, suppliers and industry analysts to maintain awareness of best practice in information security.

4. Information System Security

4.1 The School operates within the law at all times.

1. Information shall be used **legally** at all times, complying with UK and European law. All users, including employees, and agents of the School might be held personally responsible for any breach of the law.

2. All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the **General Data Protection Regulation (GDPR)**. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.

3. Personal, confidential or sensitive information **shall be protected** appropriately at all times and in particular when removed from School premises either physically on paper or electronic storage devices, or when transmitted electronically outside the School or within areas of the school in which the public may be present.

4. Personal, confidential or sensitive information shall not be included in the text of e-mails to be sent outside the authority, or in files attached to them, unless these are securely encrypted or sent by secure network links. Links **must** be secure before this is used.

5. Any request for information under the **Freedom of Information Act 2000** (FOIA) shall be handled in accordance with the law and processed within 20 working days. Such requests should be directed to the School Office.

6. Information **shall not be used** in any way that might be seen as defamatory, libellous, insulting or offensive by others, Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.

7. The School shall only use **licensed software** on its computers, servers and other computing devices.

8. Information, including texts, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of **copyright.**

9. Computers and mobile devices may not be connected to the school network, both physically or wirelessly, without specific permission from the Headteacher/ICT Technical Staff. Nor shall any personally owned or non-school equipment be connected to the school computer network or to any school owned equipment, whether on the school's network or not, without written permission from the Headteacher. Only schools encrypted flash drives to be used, any brought in with homework on or a visiting trainer must be scanned before use.

10. Portable media may not be used without specific permission from the Headteacher/ICT Technical Staff.

11. Unapproved system utilities and executable files will not be allowed to be installed or attached to emails.

12. No software will be installed on or removed from Woodlands Primary School equipment without permission from ICT Technical Staff.

13. Users shall not interfere with the configuration of any computing device without approval.

14. School equipment, facilities and information shall be used only for school's business purposes, unless written permission of line management has been obtained.

15. School equipment, facilities and information must never be used for personal gain or profit nor for electronic harassment of any kind or any action which may be to the detriment of Woodlands Primary School.

16. School equipment, facilities and information shall not be used for private or personal interests or business, where such use is deemed to be excessive or unreasonable, especially in the use of Internet or electronic mail services. Nor shall resources be wasted (e.g. people, capacity, computer).
17. Files will not be removed from a shared area without specific permission, unless the retention period for the document has expired.

18. Staff and governors must not log onto the school's network using someone else's user credentials (id), name and password.

19. Personal data (eg. personal photos or any data not work related) must not be stored on school servers without specific permission from the Head Teacher or ICT Technical Staff.

20. Staff and governors must log off if they are leaving the computer/room for a longer period, so that other staff and governors can log in and access the network if they need to. If a number of staff or governors are logged into a single machine it will slow it down significantly.

21. Unacceptable use of the school network may include, but not be restricted to: - Wasting of resources (e.g. people, capacity, and computer).
    - Alteration or destruction of the integrity of computer-based information.
    - Compromising the privacy of users or confidentiality of data.
    - Protect information (including paper and electronic resources).

22. School will ensure all personal data is fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with data protection legislation - GDPR.

23. School will ensure the confidentiality, availability & integrity of information, protecting it against unauthorised access and modification.

24. School will ensure staff and governors receive appropriate security training and guidance.

25. School will ensure legislative and regulatory requirements are met.

4.2 Access to information shall be controlled

1. The requirements for **confidentiality**, **integrity**, **availability** and **accountability** shall be determined for all information, from creation to deletion.
2. Structured **information security risk assessment** shall be used to determine the appropriate security controls required to protect information, which are proportionate to the risks to the information and information systems. This risk assessment shall be done as part of system and process development. The effort expended on risk assessment and the amount of formal documentation required shall be proportionate to the perceived risks to the information and the impact of a breach of its security.
3. Access to information shall be **authorised** by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required **before** access is granted to certain information systems and facilities.
4. There shall be adequate **separation** of functions for tasks that are susceptible to fraudulent or other unauthorised activity; Audit shall be consulted for advice on this.
5. Information users shall not attempt to access information to which they do not have **authority**.
6. Information users shall keep personal **passwords** confidential at all times.
7. **Agreements and contracts** with external business partners and suppliers shall include the requirement to adhere to this policy, where there is relevance to do so.
8. All **equipment**, including network equipment, attached to the School's computer network shall be approved by the Head Teacher **before** connection.
9. School equipment, facilities and information shall be used only for the School's **business purposes**, unless written permission of line management has been obtained. School equipment, facilities and information must never be used for personal gain or profit.
10. **Non-school** or **personally owned** equipment or storage devices shall not be connected to the School computer network or to any School-owned equipment, whether on the School's network or not, without written permission from the Head Teacher. Only Schools encrypted flash drives to be used, any brought in with
11. All information about the **security arrangements** for School computer and network systems and structured manual filing systems is confidential to the School and shall not be released to people who are not authorised to receive that information.

4.3 The availability of information shall be protected

Business continuity plans shall include all aspects of the School's **infrastructure**, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.

4.4 The integrity of information shall be maintained

1. A named individual should have operational responsibility for the ICT systems and procedures.
2. The accuracy and completeness of information, including structured manual filing systems, processing methods and computer software shall be **protected** from unauthorised modifications. Users shall not attempt unauthorised modifications.
3. Users shall use only the **officially provided or approved facilities and systems** to access School information.
4. Users shall not interfere with the **configuration** of any computing device without approval.
5. Update regularly all devices, which are subject to the threat of malware and viruses, with malware and antivirus scanning software.
6. Update regularly all devices, which are subject to the threat of **security vulnerabilities** with appropriate security patches.

5. Monitoring of the Information Security Policy

The use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure that this policy is adhered to and to detect and investigate unauthorised use of information
- To maintain the effectiveness, integrity and security of the computer network
- To ensure that the law is not being contravened
- To protect the services provided by the School and Council to the public and protect the integrity and reputation of the School and Council **All monitoring shall be:**
  - ✓ Fair and proportionate to the risks of harm to the School information and reputation
  - ✓ Undertaken so as to intrude on users' privacy only as much as is necessary
  - ✓ Carried out similarly regardless of whether the user is office based or working remotely
  - ✓ Carried out subject to the requirements of legislation, e.g. Regulation of Investigatory Powers Act 2000. Access to any records of usage shall be stringently controlled.

6. Review of the Information Security Policy

This policy shall be reviewed on a regular basis and at least annually. This policy and its associated policies, processes, procedures and guidelines shall be updated according to:

- Internally generated changes e.g. changes in service strategy, organisation, locations and technology
- Externally generated changes e.g. changes in legislation, security threats, security incidents, recommended best practice and audit reports
- All changes shall be approved by the Head Teacher and School Governors and be made available to everyone to whom it applies.

7. Information Security – General

Visitors on-site

All visitors must sign in and sign out. All staff and governors should be vigilant about the lanyard system. Green lanyard means - Approved and DBS checked visitors: parents, counsellors, contractors as detailed on list held in Acorn building. Do not require supervision with the children.
Red lanyard means - Parents, counsellors, contractors, those attending meetings and any personnel not shown on list. This includes those part way through DBS checking. MUST BE SUPERVISED and never left alone with the children or to wander around the building.

Emails

Emails sent to external organisations that are work related must be sent from a school email address.

Staff and governors must not let anyone else use their account nor share their password, in school or at home.

Personal, confidential and sensitive information sent to recipients external to the school must be encrypted.

Staff and governors must use their school account for all emails relating to school matters.

Staff and governors personal e-mail addresses should not be accessible to pupils or parents.

When teachers are responding to emails from parents/carers, responses should be courteous and brief, with the purpose of setting up a meeting. Sensitive issues should not be communicated via email.

Any e-mails sent between staff and parents/carers should be sent through their school Account.

Staff and governors are provided with an email address by Woodlands Primary School. This may be used for any legitimate educational or work related activity. Staff and governors should use the email in accordance with the following guidelines and are reminded that the School retains the right to monitor email communications at any time if this is deemed necessary.

The sending or receiving of messages which contain any inappropriate material is strictly forbidden. Messages relating to, or in support of any illegal activities may be reported to the authorities.

Whilst it is possible to attach files to an email message, staff and governors are advised that that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 7Mbytes in size are generally considered to be excessively large and staff and governors should consider using other methods to transfer such files.

File attachments must not be opened or downloaded unless staff and governors are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the School network.

Staff and governors should not send personally identifiable information by email, as it is not a secure medium.

Huge amounts of information are sent by email, within and across agencies. Whilst internal messages are generally secure (e.g. within organisations), those sent to external addresses are not considered secure enough for personal information. Personal information must be sent by other methods, some of which are outlined in this section.

When sending personal information via email, staff and governors should:

- ensure all recipients need to receive the information - think twice before responding to a group email or copying others in;

- confirm the name, department and email address of the recipient;

- use a flag to mark the message 'confidential'; do not include personal or confidential information in the subject field;

All student related emails will be automatically deleted after 6 months (except in special circumstances).

Passwords

All staff and governors have their own unique username and private passwords to access school systems. Staff and governors are responsible for keeping their password(s) private. Passwords must always be kept private and not shared with anyone under any circumstances, including with supply staff, governors and volunteers.

If a password is compromised the school should be notified immediately and the password changed.

Staff are required to change their work, SIMs and Target Tracker password at regular intervals.

Users shall not attempt to access information to which they do not have authority.

Staff and governors must never reveal their password to anyone else or ask others for their password.

It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lowercase letters, numbers and other punctuation characters (a minimum of 8 required for school password).

If a member of staff or a governor forgets their password, they should request that it be reset via ICT Technical Staff.

"Remember password" feature must never be used.

Password protection and encryption are not necessary for information shared between staff and governors within a secure platform (e.g. within the school) or where secure email is used.

Computers must never be left unattended while using any personal data – staff and governors should lock their workstation when they leave the computer – this will normally require a password to reopen.

Personal information sent to an external recipient should be sent in a password protected file.

Staff and governors must always save the password protected version of documents as a new file and retain the original safely. IT Technical Staff will not be able to open password protected or encrypted documents without the password.

Further general email rules can be found in the "Security Checklist for Staff" on Staff Public/GDPR folder.

SharePoint

Woodlands Primary School uses SharePoint as our document management platform which allows us to set up a centralised, password-protected space for document sharing.

USB Memory Sticks

USB memory sticks have a very large capacity and therefore pose a considerable security risk if they are lost, stolen or abused. Woodlands Primary School only use school provided Memory Sticks. Schools are required to make a policy decision stating if they endorse their use. Memory sticks storing sensitive information should be encrypted and only used where a strong business case can be applied.

Laptop Computers

Laptop computers are issued to teaching staff, governors and support staff as required, subject to availability. Laptops remain the property of Woodlands Primary School all times, and their usage is subject to the following guidelines:

The equipment remains the property of Woodlands Primary School at all times and must be returned to the School at the end of the lease agreement or contractual period.

Maintenance of the equipment is the responsibility of Woodlands Primary School. All maintenance issues must be referred to the ICT Department, through the usual channels.

All installed software MUST be covered by a valid licence agreement held by Woodlands Primary School

All software installation MUST be carried out by the ICT Department in accordance with the relevant licence agreements.

No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.

Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. This should be done at least weekly.

The user of the equipment is responsible for all personal files and data stored locally on the equipment. Backup of the data is the responsibility of the user. Laptops are backed up to the server when on site.

The user of the equipment must not encrypt any data or password protect any files so as to ensure future usage of the equipment, other than in accordance with this policy.
Woodlands Primary School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

From time to time, it may be necessary for the ICT Technical Staff to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

Cameras/Digital Devices

Woodlands Primary School has a strict Photography and Filming Policy which can be found on our website.

Only cameras owned by the school may be used at school and on school trips. Parents on school trips Only use school owned cameras**.**

Files on school cameras are never downloaded onto devices not owned by the school.

Cameras are locked away, at school, at the end of each day, unless being used on a residential trip.

Images may only be stored on school based devices and not on devices kept at home.

Data Security and Retention

All data stored on the Woodlands Primary School network is backed up daily and backups are stored for up to at least two weeks. If files are accidentally deleted IT Staff should be informed immediately so that they can be recovered. Currently, a full backup of all data on the network is taken at the end of each school year. The yearly backups are stored for three years.

Woodlands Primary School operates a cloud based system in which resources are retrieved from the internet through web-based tools and applications, as opposed to a direct connection to a server at the school. As such Woodlands Primary School must consider the privacy implications of such a system.

Please refer to the TEAMS Data Protection Impact Assessment (DPIA). A DPIA is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Data Encryption

All data that is taken off-site by staff and governors must be secured by a method of encryption. This means that the data cannot be read or used by anybody else, should it be lost or stolen.

For advice on encryption please consult IT Staff. All school-provided staff laptops and USB memory sticks that are taken off-site will be secured with either a software or hardware encryption method before issue. It may not be possible to encrypt personal storage devices.

Internet and Email

Content Filtering

Woodlands Primary School provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. Staff and governors should immediately inform IT Technical Staff if they discover any websites containing inappropriate or offensive content so that they can be filtered.

External Services

Webmail

Webmail provides remote access to an email account from home or anywhere with an Internet connection. Staff and governors should use email in accordance with the following guidelines and are reminded that Woodlands Primary School retains the right to monitor email communications at any time if this is deemed necessary. It is strongly recommended that webmail is not used on public or open networks as security cannot be guaranteed.

Webmail is provided for use of Woodlands Primary School staff and governors only. Access by any other party is strictly prohibited.

Using Webmail signifies that the user is an employee of Woodlands Primary School and that authorisation has been granted to use the system by the relevant School authority.

Security guidelines must be observed at all times. Passwords must never be revealed.

File attachments must be treated with caution. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the computer. Files must not be opened or downloaded unless staff and governors are certain of both their content and origin. Woodlands Primary School accepts no responsibility for damage caused to any external equipment or software as a result of using the Webmail service. The rules that apply to Email are also to Webmail.

Privacy and Data Protection

Security

Staff must never attempt to access files or programs to which they have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

Report any security concerns immediately to ICT Staff.

Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with Kent County Council Disciplinary Procedures for Local Government Services Employees.

Mobile Technologies

For reasons of safety and security staff, governors and volunteers should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. If a member of staff or a governor is sent inappropriate material e.g. images or videos it must be reported immediately.

Use of WiFi, iPads and Tablets, Mobile Devices

Mobile devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

Working From Home

Staff and governors always use an encrypted device to transport personal and sensitive information out of school. Any USB stick used for personal or sensitive school information must be a school provided encrypted stick.

Staff and governors always ensure that any school laptop taken home is encrypted, unless only remote access is used and no school information is stored on the hard drive.

Staff and governors never store personal or sensitive information or school owned mobile devices in the car.

Support Services

All ICT hardware and software maintenance and support requests should be submitted to the ICT Technical Staff using one of the following methods:

Telephone the ICT Suite – Brian Clark on extension 228

Email – ict@woodlands.kent.sch.uk

In person at the ICT Suite on the Upper Hub.

Woodlands Primary School will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

Software Installation

The ICT Staff assumes responsibility for all software installation and upgrades. Staff and governors may request the installation of new software packages onto the network, but this will be subject to the following:

Software cannot be installed on the School's network without a valid licence agreement. This must be supplied with the software package.

Licensing terms of the software package must be checked carefully to ensure that it is suitable for use on the School network. A relevant and valid licence agreement document will be required before any software packages can be installed.

All software installation media and licence agreements are held centrally within the School to aid in licence tracking and auditing. Installation media cannot normally be released except by special agreement.

When purchasing new software for use on the School network, suitability, compatibility and licensing terms must be checked with the ICT Technical Staff. Once software has been authorised by the ICT Technical Staff purchase orders should be authorised by the budget holder for the respective department.

Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the School will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, nondeliveries, misdeliveries or service interruptions caused by the system or elements of the system, or errors or omissions. Woodlands Primary School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Auditing ICT Equipment

Woodlands Primary School has an accurate and up to date inventory of all ICT assets including mobile devices and software. An inventory including who it is assigned to is essential when investigating any lost or stolen items. This will also ensure that you can verify the equipment e.g. USB. Memory Sticks are the property of the schools. All school equipment should have an asset sticker.

Cloud Computing

Cloud computing is defined as access to computing resources, on demand, via a remote network. Woodlands is aware that processing information in the cloud means we may encounter risks to data protection and we take all the necessary precautions.

The processing of certain types of personal information could have a greater impact on individuals' privacy than the processing of others. With this in mind, we review the personal information we process and determine whether there is any data that should not be put into the cloud. This may be because specific assurances were given when the personal information was collected.
Often the question may not be whether the personal information should be put into the cloud but what the data protection risks are and whether those risks can be mitigated.

8. Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the GDPR. Woodlands Primary School have taken all the necessary measures to protect records and can ensure that:

- We can demonstrate compliance with the law and avoid data loss incidents;

- In the event of a major incident, we can stay open and will at least have access to its key administrative and teaching records.

An Information Security Policy should incorporate a Business Continuity Plan and should deal with records held in all media across all school systems:

- Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images).

- Hard copy (including but not limited to paper files, plans)

1. Digital Information

In order to mitigate against the loss of electronic information Woodlands Primary School

a. Operates an effective back-up system

We undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Where possible these backups are stored in a different building to the servers and if possible off the main school site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. Woodlands Primary School operates a cloud based system.

b. Control the way data is stored within the school

Personal information is not stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff and governors do not hold personal information about students or other staff and governors on mobile storage devices including but not limited to memory sticks, phones, CD, DVD or portable hard drives.

c. Maintain strict control of passwords

We ensure that data is subject to a robust password protection regime with users changing their passwords regularly. Staff and governors do not share passwords and follow the regulations laid out on our “Checklist”.

d. Manage the location of server equipment

We ensure that the server environment is managed to prevent unauthorised access.

e. Ensure that business continuity plans are tested

We test restore processes on a regular basis to ensure that the first time we identify a problem with the backup is not the first time we need to retrieve data from it.

2. Hard Copy Information and Records

Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

a. Fire and flood

The cost of restoring records damaged by water can be high but a large percentage may be saved, fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all our vital information is stored in metal filing cabinets and drawers. Vital records are never left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard are raised at least 2 inches from the ground. Physical records are never stored on the floor.

b. Unauthorised access, theft or loss

Staff and governors are encouraged not to take personal data on staff, governor or students out of the school unless there is no other alternative. Records held within the school are kept in lockable cabinets. All archive or records storage areas are lockable and have restricted access. Where paper files are checked out from the archives we log the location of the file and the borrower, creating an audit trail. We follow strict disposal guidelines.

c. Clear Desk Policy

Our clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood damage. Our clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate).

3. Disclosure

Staff and governors understand importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Staff and governors know that where they intend to share personal information with a third party that they have considered the requirements of the GDPR.

4. Risk Analysis

Woodlands Primary School undertakes a business risk analysis to identify which records are vital to school management and these records are stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks. Woodlands Primary School has developed an Information Asset/Risk Register which can assist with this process.

9. GDPR

Woodlands Primary School is fully compliant with the **General Data Protection Regulation (GDPR)**

- The GDPR ensures that information held about data subjects (staff, governors and pupils) is used for specific purposes only. These rules apply to everyone in the school.

- The GDPR covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about all individuals in the school. The GDPR applies to paper and electronic files.

The Principles of the GDPR state that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Kept no longer than necessary.
- Processed in accordance with data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Woodlands Primary School has a Data Breach Procedure in place – please see separate Policy.

10. Further reading:

Woodlands Acceptable Use Policy
Woodlands GDPR Checklist for Staff
Woodlands Data Breach Reporting Procedure Policy
Woodlands GDPR & Data Protection Policy
Woodlands GDPR Staff Awareness Training
Woodlands Online Safety Policy

11. Declaration

I am wholly committed to this Information Security Policy, and hereby state that it is the responsibility of every individual employee of the company to ensure that all security plans, standards, procedures, work instructions and actions fully meet with agreed company and customer requirements.

Signed by:

V Lonie
Headteacher _____Date: _____

Document History Table

Document History	
Date	**Summary of changes**
May 2018	Document created
September 2018	Changes made – IT Staff replaced by BC
October 2019	Annual Review V Lonie name added
November 2020	Annual Review
May 2021	No changes