Document Owner and Approval

Mrs A Allnutt is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the School's policy review schedule.

Date: October 2025

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial issue	06.05.18
2	Corrected spelling of iPads. Added bullet point about emails not containing personal opinions about other individuals and descriptions must be kept in a professional and factual manner.	23.08.19
3	Formatting amendments	03.08.22
4	Formatting amendments and included password policy	30.08.24
5	Incorporated the Bring Your Own Device, Homeworking and Clear Desk policies as respective appendices to the Acceptable Use Policy and Agreement document	01.09.2025

Acceptable Use Policy and Agreement (Including Bring Your Own Device, Homeworking and Clear Desk Policy Appendices)

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure;
- Define and identify unacceptable use of the School's ICT systems and external systems;
- Educate users about their data security responsibilities;
- Describe why monitoring of the ICT systems may take place;
- Define and identify unacceptable use of social networking sites and school devices; and
- Specify the consequences of non-compliance.

This policy applies to staff members, governors and all users of the School's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to Mrs A Allnutt.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems, unless in accordance with the Bring Your Own Device Policy (see Appendix A). Users must not try to install any software on the ICT systems without permission from Mrs A Allnutt, Headteacher and the ICT Manager,

Mr Green. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

Mr Green is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Network Access and Security

Users are not permitted to make any physical alteration either internally or externally, to the School's computer and network hardware.

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of staff for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to James Green as soon as possible.

Users should only access areas of the Schools computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the School ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the School ICT systems or cause difficulties for any other users.

School Email

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

Where email is provided, it is for academic and professional use with reasonable/no personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy. The School's email system can be accessed from both the School

computers and via the internet from any computer. Wherever possible, all School related communication must be via the School email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
  - Email encryption;
  - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Internet Access

Internet access is provided for academic and professional use with reasonable/no personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to Mrs A Allnutt.

Therefore, staff must not access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

iPads

The School encourages the use of iPads for taking class photos. However, staff should be aware of the following guidelines:

- Photos should only have the pupil's name if they are on display in school only. Photos for the website or press must only include the child's first name.
- The use of personal iPads or similar in school is not permitted.
- All photos should be downloaded to the School network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

Any files stored on removable media must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No school data is to be stored on a home computer or un-encrypted storage device.
- No confidential or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Social Networking

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.

- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.
- Members of staff will notify the Headteacher if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos which show pupils of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or the profession into disrepute.
- Users must not give students access to their area on a social networking site (for example, adding a student as a friend on Facebook). If in exceptional circumstances, users wish to do so, please seek advice from the Headteacher.

The School may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the ICT Manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy or any other school policy;
  investigate a suspected breach of the law, this policy or any other school policy.

Mobile Phones

Mobile phones are permitted in school with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard.
- Personal mobile phone cameras are not to be used on school trips. The School provides school iPads for this purpose.
- All phone contact with parents regarding school issues will be through the Schools phones. Personal mobile numbers should not be given to parents at the School.
- Staff can use their personal mobile to contact the school whilst on a school visit.

Use of WhatsApp

WhatsApp is not permitted for use on School issued devices. Members of staff are able to use WhatsApp on their own devices for personal communication. However, when communicating with staff members in connection with school matters, no pupil or parent personal information which could include categories of personal data must be used or shared.

Failure to Comply with Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Monitoring of the ICT Systems

Any unauthorised use of the School's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Acceptable Use Agreement

To be completed by all staff

As a school user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the School rules (set out within this policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the Headteacher.

I agree to report any misuse of the network to the Headteacher and ICT Manager. Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the ICT Manager. Finally, I agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher.

Specifically, when using school devices:

- I must not use these devices for inappropriate purposes;
- I must only access those services for which permission has been granted;
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed ..... Date .....

Print name .....

Appendix A – Bring Your Own Device Policy

Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This is intended to protect the security and integrity of the School's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this appendix includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

Acceptable Use

The School embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose.

However, by accessing the School's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

All employees must agree to the following terms and conditions in order to be able to connect their devices to the company network:

- All staff who wish to use their own devices to access the School's network must sign and return the statement at the conclusion of this appendix.
- When in School, staff should connect their device via the School's wireless network for security.
- When out of School, staff can access work systems like their email or online learning platforms only via their mobile phone using the Authenticator app where necessary.
- All internet access via the network is logged and as set out in the Acceptable Use policy above, employees are blocked from accessing certain websites whilst connected to the School network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the Headteacher. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.
- If approved to use a personal device, you should upload any pictures, video or sound recordings to our school network and delete from personal devices.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- USB's can be used, however, no personal data must be stored on them unless the device is password protected.
- WhatsApp is not permitted for use on School issued devices. Members of staff are able to use WhatsApp on their own devices for personal communication. However, when communicating with staff members in connection with school matters, no pupil or parent personal information which could include categories of personal data must be used or shared.

Non-acceptable Use

- Any apps or software which are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to the School;
  - Harass others;
  - Act in any way against the School's Acceptable Use policy and other safeguarding and data related policies.
- Technical support is not provided by the School on the user's own devices.
- Storing school data on personal devices is not allowed. This includes forwarding school emails to your personal email address.

Devices and Support

- School tablets only (iPad's) are allowed to be used.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software and security tools, before they can access the network.
- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the School network.

Security

- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected) and maintaining that information.
- The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
- Staff are prevented from installing email apps which allow direct access to School emails without use of a login/password.
- If information is particularly sensitive, then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.
- In the event of any loss or theft of personal data/device, this must be reported immediately as a data breach in accordance with the School's Data Breach policy.
- The School may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).
- Staff are not permitted to share access details to the School's network or Wi-Fi password with anyone else.

Disclaimer

- The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.
- The School reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the appendix as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

I confirm that I have read, understood and will comply with the terms of the Bring Your Own Device appendix when using my mobile device to access the School network.

Signed: .....

Date: .....

Print Name: .....

Appendix B - Home Working Policy

Scope and Definitions

This appendix applies to all staff who work from home and/or use or access School systems or information from home or while working remotely. This includes individuals who are given access to the School networks and School data (including governors, students, visitors, volunteers, contractors and third parties). It applies to information in all formats, including paper records and electronic data.

Remote working means working off the School site. This includes working while connected to the School's networks.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

This appendix does not envisage home, or remote, working from outside the UK, as this would involve significant legal and practical issues, affecting both you and the School. If you wish to work from a location outside of the UK, you must obtain prior permission from Mrs A Allnutt, Headteacher.

Homeworking may be requested by staff on occasion, but must be agreed by the Headteacher.

This appendix does not form part of any contract of employment and the School may amend it at any time.

Awareness of Risk

Working from home presents both significant risks and benefits.

Staff may have remote access to information held on secure School servers but without the physical protections available in School. Without the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to data as well as a risk of loss or destruction of data. There are also greater risks posed by information "in transit" (i.e., moving data between office and home).

The risks posed by working from home can be summarised under three headings:

- Reputational: the loss of trust or damage to the School's relationship with its community;
- Personal: unauthorised loss of or access to data could expose staff or students to identity theft, fraud or significant distress; and
- Monetary: regulators such as the ICO can impose financial penalties and those damaged as a consequence of a data breach may seek redress through the courts.

Roles and Responsibilities

The decision as to whether to allow partial or full-time homeworking in relation to any given role rests with management.

Any member of staff working from home is responsible for ensuring that they work securely and protect both information and School-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting staff adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example, monitoring or supervision).

Failure to comply with this policy may result in disciplinary action.

Key Principles of Homeworking

Staff working from home must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below: -

i. To adhere to the principles of the Data Protection Act 2018 and the School's Data Protection Policy in the same way as they would if they were working in School.

ii. Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).

iii. No other members of the household should know or be able to guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g., in a locked drawer or in a secure password protected database). Passwords should never be left on display for others to see.

iv. Automatic locks should be installed on IT equipment used to process School information that will activate after a period of inactivity (i.e., computers should automatically lock requiring you to sign back in after this period of time).

v. IT equipment used to process and store School information in the home must be kept in a secure place where it cannot be easily accessed or stolen.

vi. Portable mobile devices used to process and store School information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.

vii. IT equipment in the home used to process School information should not be used where it can be overseen by unauthorised persons.

viii. It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using this equipment.

ix. Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.

x. All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating the sending of emails are outlined in the School's Acceptable Use Agreement.

Staff should always use school email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that their caller ID is blocked.

xi. Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the ICT Manager immediately.

xii. To adhere to the School's Data Retention Policy and ensure that information held remotely is managed according to the data retention schedule. Data should be securely deleted and destroyed once it is no longer needed.

xiii. If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the School and follow the School's guidance on the safe use of video conferencing.

xiv. To be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.

xv. Staff should not access inappropriate websites on School devices or whilst accessing School networks.

xvi. Staff who have been provided with School-owned IT equipment to work from home must:

a. only use the equipment for legitimate work purposes;

b. only install software on the equipment if authorised by the School's IT support. Please note that this includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins;

c. ensure that the equipment is well cared for and secure;

d. not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log in passwords or access credentials with them;

e. not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the School);

f. not collect or distribute illegal material via the internet;

g. ensure anti-virus software is regularly updated; and

h. to return the equipment securely at the end of the remote working arrangement.

xviii. Staff who process School data on their own equipment are responsible for the security of the data and the devices generally and must follow the School's Bring Your Own Device Policy and Acceptable Use Policy. In particular:

a. Where possible, devices must be encrypted;

b. An appropriate passcode/password must be set for all accounts which give access to the device. Passwords must be of a complex nature (a mix of letters, numbers and special characters) and must not be shared with others;

c. The device must be configured to automatically lock after a period of inactivity (no more than 15 minutes);

d. Devices must remain up to date with security software (such as anti-virus software);

e. The theft or loss of a device must be reported to IT services just in the same way as if a School-owned device were lost;

f. Any use of privately-owned devices by others (family or friends) must be controlled in such a way as to ensure that they do not have access to School information. This will include school emails, learning platforms and administrative systems such as SIMS;

g. Devices must not be left unattended where there is a significant risk to theft;

h. The amount of personal data stored on the device should be restricted and the storing of any sensitive data avoided;

i. Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks;

j. If the device needs to be repaired, ensure that the company used is subject to a contractual agreement which guarantees the secure handling of any data stored on the device;

k. Appropriate security must be obtained for all School information stored on the device (including back up arrangements) and there must be secure storage for any confidential information;

l. Care must be taken with file storage. Any school related work should be stored on the School network area. No school data should be stored on a home computer or on an un-encrypted storage device (such as USB stick);

m. The School may require access to a privately owned device when investigating policy breaches (for example, to investigate cyber bullying);

n. All data must be removed from privately-owned devices when it is no longer needed or at the request of the School; and

o. Devices must be disposed of securely when no longer required.

xix. Staff are responsible for ensuring the security of School property and all information, files, documents, data etc within their possession, including both paper and electronic material. In particular, physical data (i.e., paper documents, which includes documents printed at home) must be secured and staff must ensure that:

a. Paper documents are not removed from the School without the prior permission of the Headteacher. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular the information is not to be transported in see-through bags or other un-secured storage containers;

b. Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport);

c. Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed;

d. Paper documents are collected from printers as soon as they are produced and not left where they can be casually read;

e. The master copy of the data is not to be removed from School premises;

f. Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in School;

g. Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them; and

h. Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

xx. Any staff member provided with School devices must not do, cause or permit any act or omission which will avoid coverage under the School's insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the staff member should consult their line manager immediately.

xxi. All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any School-owned IT equipment or data immediately to Miss C Saunders in order that appropriate steps may be taken quickly to protect School data. Failure to do so immediately may seriously compromise School security. Any breach which is either known or suspected to involve personal data, or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Appendix B (1) – Homeworking Guidance Handout for Staff

Disclaimer:

- Staff are expected to use School owned and privately owned devices in an ethical manner at all times and adhere to the School's procedure as outlined above.
- The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this procedure.
- The School reserves the right to disconnect devices or disable services or access to services without notification.

I confirm that I have read, understood and will comply with the terms of this Home Working Procedure.

Signed.....

Date.....

Print Name.....

Appendix C – Clear Desk Guidance

Introduction

The School aims to implement and maintain data protection measures to ensure that personal data is secured away appropriately to assist in the reduction of risk of unauthorised access, loss and damage to information.

This guidance checklist is designed to give staff assistance on how to secure personal information (both paper and electronic). This guidance applies to all staff including temporary and agency staff.

Good Practice

Staff must abide by the following practice points when handling personal data.

Leaving a room

Whenever a room is unoccupied for a short period of time, you should do the following:

- Lock your computer (windows L).
- Ensure there is no personal data left face up on your desk that pupils/adults could see.

Whenever a room is unoccupied for an extended period of time, you should do the following:

- Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes mass storage devices such as USB drives and hard drives or laptops and iPads.
- Draws should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
- Devices should be screen locked and locked away.
- The SENDCo office should be locked when leaving the room and all other offices locked at the end of the day.

Confidential waste

- All wastepaper which contains sensitive or confidential information must be disposed of either by using the school's onsite secure disposal (shredders) or placed in the designated confidential waste bins. The confidential waste bins should be kept in secure areas, away from students.
- Under no circumstances should this information be placed in regular wastepaper bins.
- If the school destroy large scale files such as pupil files or HR records, they should be recorded on the data destruction log.

Computer screens

- Devices such as iPads/laptops/Chromebooks/tablets/USB sticks must be locked away at the end of the day.
- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the workday.
- Computer/laptop screens are to be locked when left unattended.
- An appropriate passcode/password must be set for all accounts. Passwords must be complex (a mix of letters, capital letter, numbers and special characters) and must not be shared with others.
- Some screens in offices will have privacy screens to prevent people accidentally viewing information that they are not supposed to see.
- Devices are configured to automatically lock after a period of inactivity.

Displays

- Passwords should not be left in open areas which are visible to others.
- Sensitive or confidential personal data displayed in classrooms should not be left visible or displayed to unauthorised persons.
- Personal data (including but not limited to seating plans, allergy details and student lists) shall be stored in folders or in secure places.
- When sharing screen to the class, staff should ensure that no personal data is shared on the projector. If this happens, staff need to report this to Miss C Saunders as this will be considered a data breach.
- Before displaying any names and photos, the School will ensure that the student/parent has provided consent.
- The School will limit the amount of data on displays. If names are necessary, only first names will be used.

Taking data offsite

- You are responsible for the security of the data in your possession and when transporting it off site you must always take steps to keep it secure.
- Paper documents should not be removed from the School without the prior permission of the Headteacher. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular, the information is not to be transported in see-through bags or other un-secured storage containers.
- Paper documents should not be used in public spaces and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport).

- Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.
- Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.
- The master copy of the data is not to be removed from School premises.
- Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in School.
- Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them.
- Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

Printing

- Any print jobs containing personal information should be retrieved immediately.
- To release printing the school will use pin numbers.

Compliance

If you have misplaced any information, then you must let Miss C Saunders know as quickly as possible.

These guidelines will be monitored for compliance by Miss C Saunders and may include random or scheduled inspections and walkthroughs.