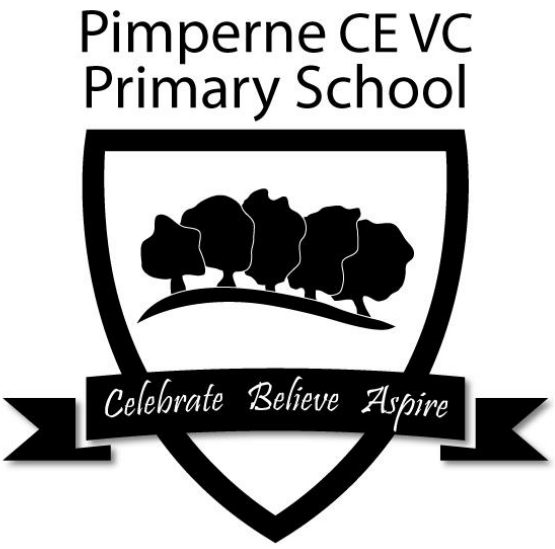


Pimperne CE VC Primary School

Staff and Volunteer Confidentiality Policy

Reviewed: Sept 2021

Next Review: July 2022

Contents:

Statement of intent

This document guides staff, volunteers and visitors on the policy and procedures surrounding confidentiality.

Staff members take a supportive and accepting attitude towards pupils as part of their general responsibility for pastoral care. It is our hope that both pupils and parents feel free to discuss worries about Pimperne Primary School, and concerns that may affect the educational progress of a pupil, with members of the school team.

This policy will be abided by at all times by staff, volunteers, visitors, pupils and parents. In order to ensure the utmost level of safety for pupils, staff members at the school have a duty to act in accordance with this policy and not share information with external agencies, other schools or individuals.

The Staff and Volunteer Confidentiality Policy has the following benefits, it:

- Ensures that important information regarding the school is not shared.
- Guarantees that financial information stays confidential and secure.
- Helps to build trust amongst staff, volunteers and external agencies.
- Supports the school's safeguarding measures.

Signed by:

FWaller	Headteacher	Date:	Sept 2021
PSlocombe	Chair of governors	Date:	Sept 2021

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

Crime and Disorder Act 1998

Equality Act 2010

The General Data Protection Regulation

Data Protection Act 2018

Education Act 2002

Human Rights Act 1998

The Education (Pupil Information) (England) (Amendment) Regulations 2019 This policy is compliant under the following case law:

The Common Law Duty of Confidentiality

1.2. This policy also has due regard to guidance documents including, but not limited to, the following:

DfE (2018) 'Information sharing'

DfE (2021) 'Keeping children safe in education'

DfE (2018) 'Working Together to Safeguard Children'

1.3. This policy operates in conjunction with the following school policies:

Data Protection Policy

Records Management Policy

Child Protection and Safeguarding Policy

Anti-bullying Policy

Freedom of Information Policy

Whistleblowing Policy

E-safety Policy

2. Definitions

2.1. For the purpose of this policy, '**confidentiality**' is an understanding that any information shared with someone in trust will only be passed on to a third party with the prior and explicit agreement of the person disclosing it.

2.2. Within this policy, a '**disclosure**' is the sharing of any private information; this term does not solely relate to child protection issues.

2.3. The term '**limited confidentiality**' refers to the disclosure of information with professional colleagues; however, the confider would not be identified except in pre-determined circumstances.

3. Roles and responsibilities

All staff members, volunteers and individuals working in cooperation with the school will:

- Uphold their responsibility and duty in relation to confidentiality.
- Ensure that information and personal details are not shared or discussed with others, except for the appropriate necessary bodies.
- Keep information regarding the school, including its pupils and parents, confidential.
- Understand and sign a confidentiality agreement and, where necessary, a responsible use of ICT agreement — as exemplified in appendix B and appendix C.

The headteacher will:

- Ensure staff understand why they must agree to the regulations set out in this policy and the documents outlined in the legal framework.
- Ensure that staff members sign confidentiality agreements.
- Remain informed of any confidentiality, safeguarding or data protection concerns within the school.
- Decide on the appropriate disciplinary procedures that will be placed upon any staff member who is in breach of their confidentiality agreement or otherwise withholds, discloses, or shares confidential information without reason.
- Ensure that this policy is kept up-to-date with all other documents, policies and statutory frameworks which operate in conjunction with this policy.

The DPO will:

- Address all concerns relating to data protection.
- Provide advice in the event of a data breach.
- Understand all relevant legislation including the Data Protection Act 2018 and the UK GDPR.
- Understand how to correctly withhold, store, move and share data.
- Ensure that the school's data is protected at all times and react quickly to any vulnerabilities.

4. Confidentiality and child protection

The school will aim to strike a balance between confidentiality and trust, ensuring the safety, wellbeing and protection of our pupils.

The contents of this section operate in conjunction with the Allegations of Abuse Against Staff Policy.

The school will always prioritise the welfare of its pupils and this will remain the primary concern when investigating an allegation which has been made against a member of staff.

The school recognises that unfounded allegations do happen, and any staff member who faces allegations relating to safeguarding concerns may find the investigation process extremely stressful. For this reason, the school will ensure that anyone who holds information relating to the investigation keeps said information confidential and will not ordinarily be shared with any other staff, pupils or parents who are not involved in the investigation.

As an employer, the school has a duty of care for its employees; meaning that anyone who possesses relevant information and is involved in an investigation will not disclose any information beyond the individuals involved.

Anyone involved in the initial assessment of an allegation will attend an allegations management meeting and share all the relevant information they have about the person who is the subject of an allegation, and about the alleged victim.

Relevant information may include files or data stored on the alleged individual's school hard drive. The school will not carry out investigations on the alleged person's personal devices; this will be carried out by the police if necessary.

Where the police are involved, the school will ask the police to obtain consent from the individuals involved to share their statements and evidence for use in the school's disciplinary process. This will be done as the investigation proceeds to enable the police to share relevant information whilst avoiding any delay to the conclusion of the investigation or court case.

The processes involved in maintaining confidentiality and carrying out an investigation will operate in line with The Education Act 2011, which made the publishing of any material illegal if it leads to the identification of a staff member in a school who has been subject to allegations by, or on behalf of, a pupil in the school.

The school will take steps to ensure that confidentiality is maintained against any unwanted publicity whilst an allegation is being investigated or considered; this will include ensuring that all staff who have access to files and data, or any other relevant form of information, sign a confidentiality agreement (see appendix A).

The school will ensure that the above restrictions on sharing information (including any speech, writing, or other communication which is exposed to any section of the public) are adhered to and will apply until:

- The accused person has been charged with a relevant offence.
- The Secretary of State publishes information about an investigation or decision in a disciplinary case arising from the allegation.

These restrictions will not be applied under the following circumstances:

- The individual who is being investigated waives their right to anonymity by going public on their own accord
- The individual being investigated provides written consent for another individual to publicly disclose the relevant confidential information
- A court lifts the reporting restrictions in response to a request to do so

Any individual, such as a parent or staff member, who discloses information to any section of the public, e.g. on a social networking site, will be in breach of the reporting restrictions if what they have disclosed could lead to the identification of the staff member by members of the public.

All external visitors will be made aware of this policy and act in accordance with it when dealing with information, particularly sensitive information, regarding the school, its pupils and parents.

The headteacher will be informed of all incidents regarding child protection concerns which are highlighted by a volunteer, parent or another external party to the school.

Staff members will be contractually obliged to immediately inform the headteacher of any concerns regarding a pupil's safety or welfare.

Any concerns raised over a child's welfare and safety will be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible.

Staff members will not be obliged to inform the police on most matters relating to illegal activity, such as illegal drugs or assaults. These will be assessed on a case-by-case basis with the support of the SLT.

5. Sharing information

The school will take the stance that all information about individual pupils is private and should only be shared with other professionals who have a legitimate need to know.

Under no circumstances will personal information about pupils, staff members or the school be passed on indiscriminately.

Under no circumstances will information regarding the school's finances be shared with anyone, other than those with a legitimate need to know.

If members of staff, volunteers or cooperating external parties share unsuitable or misrepresented information, the school withholds the right to take the appropriate civil, legal or disciplinary action.

All non-teaching staff and volunteers will report safeguarding concerns to the DSL as soon as possible and in an appropriate setting.

The DSL will:

- Understand the importance of information sharing with other schools, safeguarding partners, practitioners and any other relevant agencies or organisations.
- Understand relevant data protection legislation and regulations with particular reference to the Data Protection Act 2018 and the UK GDPR.
- Keep detailed, accurate, secure written records of concerns and referrals and understand the purpose of record-keeping.

All data will be processed and held in line with the school's Data Protection Policy. In the event of information and data being shared with external or inappropriate parties, the individual

responsible will be liable for disciplinary or legal action in accordance with the Data Protection Policy.

The DSL recognises and assures staff members with concerns about a safeguarding issue that the Data Protection Act 2018 and the UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare.

Staff members who manage or have access to the school's data will always uphold the school's obligation to process personal information fairly and lawfully, and keep the information they hold safe and secure.

The school will be open and honest with all individuals about how and why data is shared, unless it is unsafe to do so.

The school will ensure that all applicable staff have due regard to the relevant data protection principles, which allow them to share and withhold personal information. This includes:

- Being confident of the processing conditions which enable the storing and sharing of information for the purposes of safeguarding – such sensitive and personal information will be treated as 'special category personal data'.
- Understanding that the 'safeguarding of children and individuals at risk' is a condition allowing staff to share special category personal data – this includes sharing information without consent where the sharing of this information will enhance safeguarding, or solve a safeguarding issue in a timely manner.
- Withholding the provision of data in compliance with the school's obligations under the Data Protection Act 2018 and the UK GDPR – where in doubt, the school will seek independent legal advice.

Where necessary, advice will be sought from the DPO and other practitioners to ensure all data is shared correctly.

Where possible, information will be shared with consent from the data subject, unless the school is able to proceed without consent under the UK GDPR and Data Protection Act 2018, e.g. if the data subject's safety is at risk.

Individuals' safety and wellbeing will form the base of all information sharing decisions, and information will not be shared if anyone's safety or wellbeing could be compromised.

Only information that is necessary for the purpose it is being shared for will be shared.

All decisions and reasons for sharing data will be recorded by the DPO.

6. Breaking confidentiality

6.1. When confidentiality must be broken because a child may be at risk of harm, in accordance with the school's Child Protection and Safeguarding Policy, the school will ensure the following:

Pupils are told when information has been passed on

Pupils are kept informed about what will be done with their information

To alleviate their fears concerning the information becoming common knowledge, pupils are told exactly who their information has been passed on to

6.2. If confidential information is shared with the explicit consent of the individuals involved, and they are informed of the purpose of sharing the information in question, there will be no breach of confidentiality or of the Human Rights Act 1998.

6.3. In the event that explicit consent for sharing confidential information is not gained, an individual will satisfy themselves that there are reasonable grounds to override the duty of confidentiality in these circumstances before sharing the data.

6.4. The school recognises that overriding public interest is a justifiable reason to disclose information; however, permission from the headteacher will be sought prior to disclosing any information regarding the school.

6.5. Staff should act in accordance with the school's Whistleblowing Policy at all times.

6.6. Individuals who disclose information, after previously agreeing to the school's confidentiality agreement, may face further action, including legal action.

6.7. Staff in breach of this policy may face disciplinary action, if it is deemed that confidential information was passed on to a third party without reasonable cause.

7. Responsible use of ICT and technology

Every member of staff will adhere to the school's ICT Acceptable Use Policy at all times.

All staff, with particular reference to ICT technicians and staff members with access to wider files and data, will understand their obligation to use ICT systems in a responsible way and respect others' privacy and confidentiality.

Staff will understand that their use of ICT systems, email and other digital communications will be monitored and the staff responsible for monitoring such activities will not share any confidential information unless this is for the purposes of keeping children safe or any other legal complication.

Staff will never disclose their password to anyone, nor will they attempt to use another individual's account details.

All staff will immediately report illegal, inappropriate, or harmful material seen on another individual's network to the headteacher.

Anyone found accessing, copying, removing or altering any other user's files without permission will face appropriate disciplinary measures.

Communication with pupils and parents will only take place through official school systems.

The headteacher and DPO will be informed immediately in the event of a data breach on any school device.

The use of any programmes or software that attempts to bypass filtering or security systems in place at the school is strictly prohibited.

As outlined in the school's Data Protection Policy, all staff members will understand that any staff or pupil data, which they have access to, will be kept private and confidential unless the sharing of information is deemed necessary as outlined above.

8. Accessing information

8.1. In accordance with article 15 of the GDPR, personal information, such as educational records, can be shared via a subject access request (SAR).

These requests must be made in writing to the governing board and will be responded to within 15 school days if the request is regarding an educational record.

If the data being requested is not in relation to an educational record, the response must be within one calendar month.

Pupils, or the parent of a pupil, have the right to access the information that the school holds about the child in question.

Some types of personal data are exempt from the right of a SAR and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have.

Information regarding another individual must not be disclosed in a SAR.

Individual requests for non-personal information cannot be treated as a SAR but will be dealt with as a freedom of information (FoI) request.

8.2. In line with the Freedom of Information Act 2000, private data and public records can potentially be accessed through lodging an FoI request.

These requests must be made in writing to the school, stating the name and address of the requester as well as a description of the information requested.

Successful FoI requests will be responded to within 20 working days from receipt of the request, unless the request does not comply with the procedure set out in the school's Freedom of Information Policy.

The school holds the right to charge the requester a fee.

Certain information will not be shared, such as that explained in Part 2 of the Freedom of Information Act 2000.

9. Management and security of school records

In line with the school's Records Management Policy, any staff member who is responsible for or has access to files, documents or data within the school's ICT infrastructure, database

or other, is contractually obliged to maintain the security and management of such records which relate to:

- Pupils
- School management
- Finances
- Personal details of pupils or staff
- Information regarding progress and attainment which is not published on the school website

10. Monitoring and review

10.1. This policy is monitored for effectiveness by the headteacher and is reviewed annually, or where necessary in light of changes to the law or statutory guidance

10.2. A record of information which has been shared will be continuously kept up-to-date.

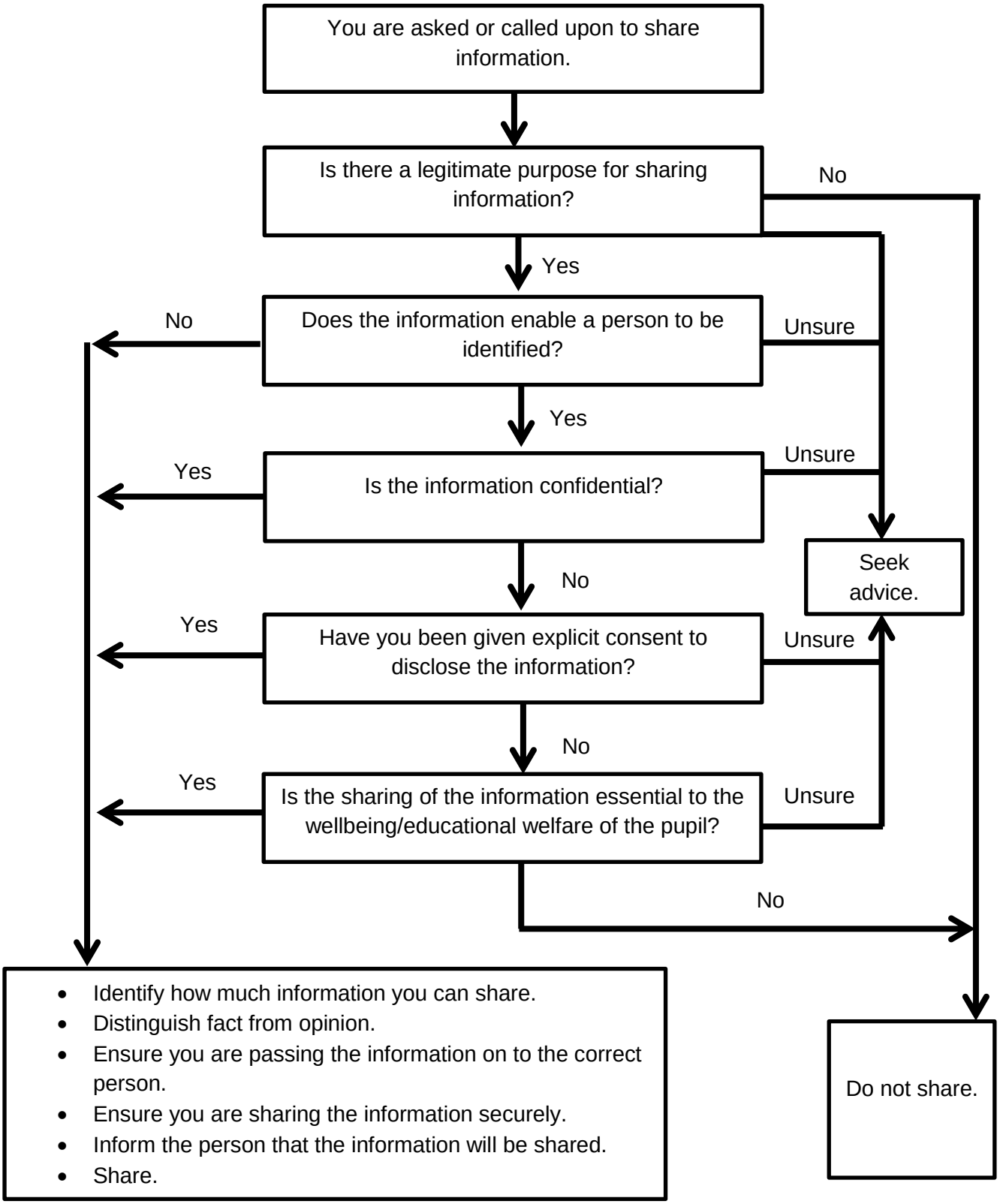
This record will state the premise of the information, whom it was shared with and the purpose for sharing it.

The record will be kept in the school office and can be accessed by all appropriate staff members.

On an annual basis, the headteacher and DSL will review the record to ensure that all reasonable measures to safeguard pupils and protect the reputation of the school are being taken.

The next review date is July 2022.

Appendix A – Information Sharing Flowchart



Notes

- If there are child protection concerns, follow the relevant procedures without delay.
- Always seek advice if you are unsure whether to share information.

Appendix B – Confidentiality Agreement

Informal confidentiality agreement

This confidentiality agreement is entered into by and between the Pimperne Primary School and all staff, whatever their role within school, for the purpose of preventing the unauthorised disclosure of confidential information in line with your duties to protect personal information, under the Data Protection Act 2018.

For the purpose of this agreement, “confidential information” will include all information or material that has or could have value, commercial or otherwise, in the business in which the disclosing party is engaged.

I declare that as a staff member of the school, I will only share or disclose information regarding the school with other professionals who have a legitimate need to know about it. I will, therefore:

- Not disclose confidential information to any unauthorised person without the discloser’s consent.
- Act in good faith at all times in relation to the disclosure of confidential information.
- Not post confidential information regarding pupils, staff, parents or other stakeholders on social media. Nor will I contribute to discussions on social media regarding the school or anyone associated with it.
- Ensure that anything I hear that questions the professionalism of a member staff or volunteer of the school is reported to the headteacher immediately.
- Ensure that if I notice anything of concern regarding the protection or safeguarding of a child, I will report it immediately to the headteacher.
- Assure that conversations of a sensitive nature regarding pupils, parents, staff, volunteers or other stakeholders take place in a private space.
- Comply with the school’s Records Management Policy when completing tasks pertaining to paperwork or online documents that include personal or sensitive information on it.
- Be fully aware that other staff, volunteers or stakeholders may have connections within the school and may overhear conversations of a sensitive nature.
- Uphold the good name and reputation of the school at all times; inside and outside of school.

I will hold and maintain the confidential information in strictest confidence for the sole and exclusive benefit of the school; therefore, I will not, without prior approval of the school, use for my own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of the school, any confidential information.

I have read and understood the school’s Staff and Volunteer Confidentiality Policy and will act in accordance with this policy at all times.

Information which may be deemed as ‘sensitive’ will not be disclosed to people where it is not wholly necessary. This includes information in relation to the following:

- Pupils of the school
- The running or management of the school

- The school's finances
- Personal details of pupils, their families or members of staff and their families
- Information regarding progress and attainment which is not published on the school website

By signing this agreement, you are agreeing to your duty to hold confidential information in confidence – this will remain in effect until the information no longer qualifies as confidential, or until the school sends written notice releasing you from this agreement, whichever occurs first.

This is an expectation of all staff. Please retain a copy of this agreement. If you have any questions or concerns, please contact the headteacher on f.waller@pimperne.dorset.sch.uk

Please sign, date and return to the Headteacher (keeping a copy fo yourself)

Date: _____

Appendix C - Responsible Use Agreement – ICT Technicians

Pimperne Primary School **Date:**

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

As our ICT technicians have greater access to our computer systems and security, the school has taken the appropriate measures to ensure our ICT technicians understand what is expected of them as they carry out their duties.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any pupils, staff or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the UK GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the e-safety officer or headteacher.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.
- I will only use recommended removable media and will keep this securely stored in line with the UK GDPR.
- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary, and which is encrypted.
- I will provide removable media to the e-safety officer for safe disposal once I am finished with it.

- I will assist in the recording and maintenance of all school software and hardware using an inventory, which I will audit on a termly basis.
- I will document all changes to software and hardware using the inventory.
- I will remove all out-of-date and 'end of life' software and detail this in the inventory.
- I will make sure all devices and user accounts are password protected.
- I will work with the firewall provider/manager to ensure the delivery of high-quality firewall protection.
- I will work with the e-safety officer to ensure the delivery of high-quality firewall protection.
- I will undertake regular malware scans on all devices to make sure they are suitably protected from the threat of infection.
- I will install and maintain mail security software to block and filter all spam and harmful emails.
- I will not remotely access any devices without first seeking authorisation from the e-safety officer – any remote access I do undertake will be documented.
- I will check the school's internet filtering software for updates to protect users from inappropriate and malicious content.
- I will ensure all new users are safely added to the school system and ensure they understand what they can and can't access.
- I will safely remove all inactive users from the school's systems to ensure no pupil or member of staff can regain access to the school network after they have left.
- I will, at the start of every school year, remind all users to update their passwords.
- I will maintain secure and safe records of user passwords to help users reset passwords where necessary.
- I will work with the DPO and, where necessary, the e-safety officer to ensure the safe and proper review, back-up and disposal of all data the school holds.
- I will not access any personal or sensitive personal data pertaining to any member of staff, pupil, visitor or other person, without the express permission of the individual in question and/or the DPO.
- I will assist with the school's helpdesk provision – ensuring timely resolutions to requests and problems, and offer updates on the status of requests.

2. Mobile devices

- I will only use school-owned mobile devices for purposes relating to the school and my role.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure personal mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use any mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.

- I will not use any mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the headteacher or e-safety officer.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the e-safety officer to erase and wipe data off my device if it is lost or as part of exit procedures.
- I will ensure all apps on mobile devices are kept up-to-date and secure – apps will only be downloaded after they have been approved and authorised by the e-safety officer.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Working at home

- I will adhere to the principles of the UK GDPR when taking work home.
- I will ensure I obtain permission from the headteacher and DPO before any personal data is transferred from a school-owned device to a personal device.

- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the DPO and e-safety officer before it is used for lone-working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's Online Safety Policy when transporting school equipment and data.
- I will ensure all school-owned devices, e.g. laptops, mobile phones and tablets, are encrypted and password protected before they are used away from the school premises.
- I will review all devices before they are used away from the premises to ensure the correct tracking software is installed – so any lost or stolen items can be retrieved.

5. Training

- I will ensure I participate in any e-safety or online training offered to me and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the e-safety officer and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.
- I will ensure all staff members and pupils receive the correct training to identify and block any potential cyber-attacks, data breaches or suspicious emails they could receive.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the headteacher.
- I understand that my use of the internet will be monitored by the e-safety officer and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.
- I will keep a record of all users who have accessed and/or tried to access inappropriate content on school devices.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed: Date:

Print name:

Headteacher's signature: Date:

Print name: