The Royal Borough of Kingston upon Thames
Southwark Diocese Board of Education

Malden Parochial C of E Primary School

Acceptable Usage Policy

Agreed: Spring Term 2021
To be reviewed annually

Ethos Statement

This is a Church of England Primary School. As such, its ethos derives from the Christian Gospel. In all that it does or aspires to achieve, the school is informed and strengthened by Christian belief and practice.

At the heart of the school's ethos is the conviction that God loves each person: that God desires the best for each person; that God longs for each person to develop their potential as human beings.

Mission Statement

In accordance with the Ethos Statement, our school will aim to provide high quality education to the children of the local community within a safe, happy and stimulating environment.

Love, Learn, Live!

Introduction

These four policy statements have been created to protect the interests of the school, its staff, pupils and governors. These conditions may be changed at the discretion of the Headteacher at any time. All staff and members of the Governing Body who wish to use school computing resources and systems are required to sign a copy of the declaration contained in this document, to be returned to the school and kept on file. Once approved by the Headteacher, access rights will be established. A record will be maintained of all users with system access. Users will be removed from this record when access is no longer required, in accordance with the Data Protection Act. Users will be advised of any changes made to these policies.

1. Acceptable Use

The computing facilities are owned by the school (this includes laptops allocated to individual staff) and their use is an entitlement for all authorised users subject to the conditions set out below:

- All computing based activity must be appropriate to a school environment
- Access to computing resources must be made via the user's authorised account and password (LGfL Staffmail)
- Users will not disclose their account name and password to any other person
- Users will always log in using their own usernames and passwords
- It is forbidden to partake in any activity that threatens the integrity of the school's facilities including the use of the internet to access inappropriate materials
- The school reserves the right to monitor the use of computing resources, emails sent or received, files held and internet sites visited at any time including examining and deleting any files held.
- Users must prepare the use of video clips and images to ensure they are appropriate before sharing with children
- Staff must always log off any computer after use

By logging on to the school's computing resources all users agree to abide by the condition above and agree not to use them to:

- Access chat room services or download files from the internet without express permission
- Publish information which could identify the user or any other person directly on any web page
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Upload, download or otherwise transmit commercial software or any copyrighted materials
- Introduce any form of computer virus into the network
- Transmit unsolicited commercial or advertising material
- Use the service to set up or run a personal business
- Post anonymous messages or send chain letters
- Broadcast unsolicited personal views on social, political or religious matters

- Represent personal opinions as those of my school or local authority
- Send pupil or staff data through unauthorised lockdowns

2. Live streaming and pre-recorded lessons

Remote learning will only take place using the platform Google Classroom.

Google Classroom has been assessed and approved for use by the Headteacher and Senior Leadership Team (SLT).

Staff will only use Malden Parochial managed accounts created using Google Classroom approved professional accounts, with learners and parents/carers.

Pupils and staff are expected to use strong passwords when accessing Google Classroom. Staff are expected to log off and lock devices when not in use.

Work submitted by pupils will be tracked using Google Classroom.

Use of any personal accounts to communicate with learners and/or parents/carers is not permitted. Staff will only use their Google email account to communicate with their class and the parents/carers.

All livestreaming will be formally timetabled; staff, parents and pupils have been provided with an overview of when these video calls will be taking place. Live lessons will be hosted on the same day and time when the school is in session.

- Livestreamed remote learning sessions will only be held with approval and agreement from the Headteacher/a member of SLT. All live lessons will be held using the Google Classroom platform.

- Staff will record children's attendance at livesteamed lessons. The lesson content, including participation, will not be recorded.

- When live streaming with learners:
  1.) contact will be made via learners' Google accounts and logins. The time and date of any live lessons will only be shared with pupils within the class.
  2.) staff will mute/disable learners' videos and microphones. There may be periods during a lesson when the class teacher will speak with pupils and also allow questions to be asked.

Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom. All participants are expected to behave in line with existing school policies and expectations.
This includes:

- Appropriate language will be used by all attendees
- Staff will not take or record images for their own personal use
- Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing
- Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session

- When sharing videos and/or live streaming, participants/ staff are required to:
  1.) wear appropriate dress.
  2.) ensure backgrounds of videos are neutral (blurred if possible).
  3.) ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds

3. Video-conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents/carers if their child is engaged in video conferencing with individuals or groups outside of the school via Google Meet. Children should always be supervised by a member of staff and a record of dates, times and participants held by the school.

4. All users also agree to:

Seek permission from the Headteacher or the Subject Leader for Computing before downloading any software

Report any inadvertent access to inappropriate websites

Transfer of sensitive data
We aim to produce guidelines for staff to minimise a breach of data during which sensitive data may be lost, become vulnerable, altered or stolen. Sensitive data is defined as any personal or confidential information that can be linked to a specific person.

With regards to sensitive data staff are expected to:

- Never create or store data which contains any client-specific information on personal devices, regardless of the intended use of the data
- Only use password protected school supplied laptops or an encrypted memory stick should they need to transport sensitive data
- Only use laptops and an encrypted memory stick as a means of transporting data on a temporary basis
- Transport data to school storage facility and delete data from laptop or memory stick as soon as it is no longer needed
- Only take sensitive physical data e.g. pupil file, home when absolutely necessary and with the express permission of the Headteacher (on an encrypted memory stick)
- Never leave sensitive data/files unattended
- Maintain the confidential nature of the data wherever that data may be e.g. car/home. (no labels visible)
- Never read or make notes on sensitive files during a journey on public transport
- Never post images relating to Malden Parochial on the internet or social networking sites

With regards to the use of emails staff are expected to be aware that:

- The content security and safe receipt of information sent by email is always the responsibility of the sender

- Emails can be the subject of interception
- Good practice includes the use of initials rather than name/s, date of birth, address etc.
- Normal non-secure email may be used for day to day communication with colleagues, third parties and other agencies where the nature of the information is not confidential.
- Any electronic communication between schools and the Local Authority which contains sensitive data must be made using a secure system called USO-FX or through the DfE portal School-to-School (S2S).
- Anonymised information may be sent through normal email only when extra care has been taken to verify the recipient. (e.g telephone call)
- Pupil specific reports and documents should not be sent as an attachment to an email, they are to be sent via USOFX or other agreed secure systems e.g. DfE, S2S portal.
- Emails should always be of a professional nature with due regard to the recipient.
- Emails containing sensitive data and/or in connection with school matters should only be created and sent by authorised staff. Sensitive data to be sent via Atomwide.

Data Breaches

On the discovery of a potential breach of data the matter should be referred immediately to the Headteacher. The Headteacher will then initiate an enquiry to ascertain the nature and scope of the breach. If it is believed that sensitive data may have been compromised then the Headteacher will contact the School's Data Protection Officer (DPO), who will give advice regarding any subsequent action.

Online safety for pupils

All adults within the school are responsible for ensuring pupils are safe when using the internet. The computing skills ladder contains information regarding when and how online safety is to be discussed and taught. Teaching staff are required to follow this scheme of work.

In addition to the scheme, teachers will discuss and explain the computing Code of Conduct appropriate to the age of the pupils being taught. Pupils from year 1 upwards are asked to sign a copy of the Code of Conduct at the beginning of each academic year. Copies of the code are displayed in the Computing Suite.

Online Safety for adults

In addition to the Acceptable Usage and Transfer of Data policies staff are required to use the computing facilities sensibly, lawfully and professionally. Training in online safety will be provided at regular intervals for all staff.

National guidance

- DfE: ‘Safeguarding and remote education during coronavirus’ (COVID-19)
- NSPCC: Undertaking Remote Teaching Safely
- National Cyber Security Centre: Video Conferencing Services
- SWGfL: Safe Remote Learning
- LGfL: Safeguarding during Covid-19

Acceptable Usage Policy

Staff Agreement

All staff within Malden Parochial CofE Primary School, must be aware of their responsibly for safeguarding when using any online technologies, such as the internet, e-mail or social networking sites.

All staff must read and sign the Staff Agreement section of this Acceptable Usage Policy on an annual basis. By doing so an example is set to the children for the safe and responsible use of online technologies. This policy aims to educate, inform and protect the adults in our school so that they are protected from any potential allegations of misconduct and know what to do in the event of inadvertent misuse.

- I know that I must only use the school's IT resources in an appropriate manner and for professional usage.
- I understand that I need to obtain permission from parents/carers before I can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images taken of the children must be appropriate and not reveal any personal information about the child. (full name, age or address)
- I have read and understood the policy statements relating to procedures for dealing with incidents of misuse.
- I will report accidental misuse to the Designated Lead for Computing. (DLC)
- I will report any incidents of concern for a child's welfare and safety to the Designated Safeguarding Lead (DSL) in accordance with procedures listed in the Safeguarding and Child Protection Policy, and the Acceptable Usage Policy.
- I know the members of staff who hold the positions of Designated Safeguarding Lead (DSL) and the Designated Lead for Computing (DLC)
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail. I know, I should use the school e-mail address and phones to contact parents.
- I know that I must not use the school system for personal use, unless previously agreed by the Headteacher.
- I know that I should complete virus checks on my laptop and other storage devices; including regularly installing updates on school devices, so that I do not inadvertently transfer viruses, especially where resources have been downloaded.
- I will ensure that I follow the Data Protection Act 2018 and have checked I know what this involves.
- I will ensure my password is kept secure and I will not disclose any security information unless to appropriate personnel. If my password is requested by a second person or organisation, I will check with the Headteacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission to use.
- I will ensure the safekeeping of school equipment if I take it off the premises and I understand I may be held responsible for any loss and damage if the school's property is misused.

- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden and I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have received a copy of Malden Parochial's Acceptable Usage Policy (staff), the Protocol for Livestreaming and the Risk Assessment. This allows reference to all online-safety issues, remote learning, livestreaming and procedures that I should follow. I understand a copy can be found on the Staff Secure Login.
- I have read, understood and agree with the Staff Agreement section of the Acceptable Usage Policy. I realise that by following these policy statements, guidelines and procedures, I will develop my understanding of online safety and my responsibility to safeguard children when using online technologies.

****

TO BE KEPT IN STAFF FILE

The computing policies covering Acceptable Usage, Transfer of Data and Online Safety have been received, read and understood.

I agree to abide by the conditions therein.

I understand that misuse of schools computing equipment or systems is a serious offence and may lead to disciplinary procedures.

User's name: ______________________________

User's signature: ____________________________

Headteacher signature: __________________________

Date: ________________________