MIDDLETON PARISH CHURCH SCHOOL

Acceptable Use/E-safety Policy

'Excellence, Truth and Grace'

RATIONALE

The primary purpose of this policy is twofold: -

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Middleton Parish Church School website; upon review all members of staff will sign as read and understood this 'E-Safety' Policy and the 'Staff Acceptable Use of ICT' Policy. A copy of the 'Pupils' Acceptable Use of ICT' Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

For clarity, this policy uses the following terms unless otherwise stated:

- **Users** - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.
- **Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian or carer.
- **School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.
- **Wider school community** – students, all staff, governing body, parents, volunteers

Safeguarding is a serious matter; at Middleton Parish Church School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed during the October Governors' meeting on an annual basis.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
- Keep up to date with emerging risks and threats through technology use.

- Receive regular updates from the Head teacher in regards to training, identified risks and any incidents.
- Chair the E-Safety Committee

Head teacher

Reporting to the governing body, the Head teacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer (or more than one), as indicated below.

Josie Jenkins (Computing Subject Leader)
Nadia Matthews (PSHE Subject Leader)

The Head teacher will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated E-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise himself/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head teacher.
- Advise the Head teacher and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that: -
The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head teacher.

Staff are to ensure that: -

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Head teacher.
- Any e-safety incident is reported to the E-Safety Officer (and an e-safety incident report is made), or in his/her absence to the Head teacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Head teacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the 'Pupils' Acceptable Use of ICT' Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the 'Behaviour' policy.

E-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff and will be made aware of how they can report areas of concern whilst at school or outside of school. This will be repeated in class on a weekly basis. The school is aware of its duty to work with the community to protect our pupils from radicalisation from extremist groups. It is known that the internet and social media have a part to play in recruiting young people. We as a staff therefore promote British Values and encourage open debate within our PSHE program. We will report any suspicious activity on our ICT systems or through child disclosure through this policy and our 'Safeguarding & Child Protection' policy.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through Parents' Evenings, school newsletters, the school website (www.middletonparishce.rochdale.sch.uk) and Twitter (@Midd_Parish) the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the 'Pupils' Acceptable Use of ICT' Policy before any access can be granted to school ICT equipment or services.

E-Safety Committee

Chaired by the Governor responsible for e-safety, Adele Bridle, the E-Safety Committee is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer pupils, parents, the E-Safety Officer, responsible Governor and others as required, the E-Safety Committee will meet on an annual basis.

Technology

Middleton Parish Church School uses a range of devices including PCs, laptops, iPads, and iPods. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – We use Fortigate Web-filtering managed by our Network Connectivity supplier, Network Connect Ltd, that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Subject Leader and E-Safety Officer are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head teacher.

Email Filtering – we use Microsoft Office 365 web-filtering that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. Where there is an ambiguity the filtering places potential unsolicited e-mail (spam) into either Clutter or Junk Mail folders of the users' inbox for them to identify and deal with.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) should be encrypted to the international standard of AES256. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB pen drives) is to be brought to the attention of the Head teacher immediately. The Head teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does <u>not</u> mean password protected.)

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and student passwords will change if there has been a compromise. The Computing Subject Leader and ICT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ICT Support will be responsible for ensuring this task is carried out, and will report to the Head teacher if there are any concerns. All USB peripherals such as pen drives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the staff 'Acceptable Use of ICT' Policy; pupils (parents) upon signing and returning their acceptance of the 'Acceptable Use of ICT' Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Home School Agreement, and is re-iterated here for clarity. All parents must sign a photo/video/ social media release slip at the beginning of each academic year. Non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Middleton Parish Church School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Middleton Parish Church School and have been appropriately risk assessed; staff and pupils are not permitted to use any other social media services within the school premises.

- Blogging on the school website – used by staff and pupils in school.
- Comments page on school website
- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. The E-Safety Officer/Head teacher will decide on the suitability of organisations/individuals to follow on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the home school agreement) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Remote Meetings
Middleton Parish Church School authorises the use of 'Zoom' to allow staff and governors to conduct remote meetings. Users will ensure that 'Zoom' is only being used in accordance with school's 'Acceptable use of ICT' policy, the 'Virtual Meeting' policy and Zoom's own acceptable use policy.

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Head teacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Middleton Parish Church School will have an annual program of training (September) which is suitable to the audience. This will link to the 'Safer Working Practices' Policy.

New staff, students and volunteers take part in an induction program in which e-safety is covered as part of Safeguarding and Safe Working Practices.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. E-safety is part of our Computing Curriculum and PSHE (Personal Social Health Education). We also take part in E-Safety Days each year. Assemblies, workshops and cross-curricular lessons are incorporated into this.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head teacher for further Continuing Professional Development.

Review Date: January 2021 Next Review: September 2021

APPENDIX A

Acceptable Use of ICT Policy – Staff

Note: All internet and email activity is subject to monitoring.
You must read this policy in conjunction with the 'E-Safety' Policy. Once you have read and understood both **you must sign this policy sheet.**

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks. Staff who are friends with parents prior to their children attending the school, should use their professional judgement when deciding whether to continue their online friendship and when considering the posts they share. In addition, staff should never have friends online who are under the age of 18, unless they are related.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support. Make sure that you log off computers when away from your desk for long periods or lock the computer if away for short periods.

Data Protection – when working from home, or off site, you should ensure that your device (laptop, USB pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device. Encrypted USB are provided by school and must be signed for in the school office.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the E-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Edit Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school and whether in work or at home.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with pupils.

School Network – all data on the local school network or wider Rochdale School Virtual Network must be kept safe and comply with associated security and data protection policies. Failure to do so could result in disciplinary actions being taken (https://intranet.rochdaleschools.org/help/documents).

NAME :

SIGNATURE : **DATE :**

APPENDIX B

Acceptable Use Policy – Pupils

Note: All Internet and email activity is subject to monitoring. The following statements apply to all digital activity, both inside and outside of school.

I Promise to:

- only use the school ICT for schoolwork that the teacher has asked me to do.
- not look for or show other people things that may be upsetting.
- show respect for the work that other people have done.

I will not:

- bring my mobile phone to school at any time, including extra-curricular events. If I bring my mobile phone to school, I will ensure that it is handed to a member of staff for safe-keeping.
- use other people's work or pictures without permission to do so.
- damage the ICT equipment; if I accidentally damage something I will tell my teacher.
- share my password with anybody. If I forget my password I will let my teacher know.
- use other people's usernames or passwords.
- share personal information online with anyone.
- download anything from the Internet unless my teacher has asked me to.
- use any form of social media in school.
- let my teacher know if anybody asks me for personal information.
- let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
- be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand that:

- some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
- that if I break the rules in this charter there will be consequences for my actions, in line with the school's 'Behaviour' policy and my parents will be told.

Signed (Parent):

Signed (Pupil):

Date:

APPENDIX C

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		

Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Inappropriate Activity Flowchart