Milldene Primary School

E-Safety Policy

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

1. E-Safety - Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Officer
- regular monitoring of e-safety incident logs
- reporting to Governors' meeting

The **Headteacher** has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the E-Safety Officer.

- The Headteacher and (at least) another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

The named **E-Safety officers** are the level 3 trained designated officers**.** It is the role of the E-Safety officers to:

- keep abreast of current issues and guidance
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- receive reports of E-safety incidents and create a log of incidents to inform future e-safety developments
- provide regular training and advice for staff
- liaise with: technical support staff; the subject leader for ICT and computing; the E-Safety governor

It is the responsibility of the **Network Manager/ICT technician** to ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply
- that users may only access sensitive information through a properly enforced password protection policy, in which passwords are regularly changed
- that any evidence of misuse / attempted misuse of the network / internet / Virtual Learning Environment / Email is reported to the Headteacher/ E-Safety Officer.

The **subject leader for computing** is responsible for providing a scheme of work for E-Safety and monitoring its implementation in consultation with the E-safety Officers.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (Appendix 2)
- they report any suspected misuse or problem to the Headteacher / E-Safety Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- passwords are changed regularly

Pupils are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy (Appendix 1)

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

2. Teaching and Learning

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- The school has a scheme of work for teaching internet skills and e safety in Computing & PSHE lessons.
- Pupils are reminded regularly of the school rules for Internet use in lessons. SMART rules are posted in the ICT suite and classrooms.
- Although the children have filtered access to the Internet, they are taught to manage risks that they may encounter out of school.
- Key E-safety messages are reinforced as part of a planned programme of assemblies.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.

3. Training

A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

4. Technical infrastructure, filtering and monitoring

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school academy technical systems.
- The server and wireless network are password protected.
- All users will have clearly defined access rights to school technical systems and devices.
- Staff will be provided with a username and secure password by the Network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every six months.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the headteacher or other nominated senior leader and kept in a secure placer.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.

5. School Website

As the school's website can be accessed by anyone on the Internet, the following will be observed to protect staff and pupils.

- The point of contact on the website will be the school's address, its e-mail address and its telephone number. Staff or pupils' home information will not be published.
- Photographs of pupils will be selected carefully and will include only those pupils whose parents or carers have given written permission prior to publication.
- Pupils' full names will not be used.
- The Head Teacher will take overall editorial responsibility and will ensure information and content is both accurate and appropriate.
- The copyright of all material must belong to the school or be attributed to the owner where permission to reproduce has been obtained.

6.Emerging technologies

Where new technologies emerge, their risks and their benefits will be assessed. Mobile communications, wide Internet access and multimedia devices present new opportunities. However, such technologies will be evaluated in order to assess risks, establish benefits and identify best practise. The school's approach will be to deny access until a risk assessment has been completed and safety has been demonstrated.

7. Pupils' Access to the Internet

Milldene Primary uses the E2BN's filtered Internet service, which will minimize the chances of pupils encountering unsuitable material. We will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards every computer screen. Members of staff will be aware of the potential for misuse and will be responsible for explaining expectations of proper use to pupils.

Parents sign an internet use agreement when they start school. (Appendix 1)

Teachers will have access to pupils' emails and other Internet files generated in school, and will check these periodically to ensure that expectations of behaviour are being met.

9. Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Others issues related to data protection are set out in the Data Protection Policy.

10. Reporting E-Safety Incidents

All incidents must be reported to the E-Safety officer who will keep a log (Appendix 3). Any serious incidents must be reported to the headteacher immediately.

To be reviewed September 2023

Appendix 1

Milldene Primary School

Rules for Responsible Internet Use

The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us to be fair to others.

Using the computers:

- I will only access the computer system with the login and password I have been given;
- I will not access other people's files;
- I will not bring in floppy discs, USB Flash drives or CDs from outside school and try to use them on the school computers without the permission of the ICT co-ordinator or the ICT technician.

Using the internet:

- I will ask permission from a teacher before using the internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and monitor the internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

Using e-mail:

- I will ask permission from a teacher before checking my e-mail;
- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I send or receive may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

Signed: Date:

Appendix 2

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Susan Locke, Headteacher.

- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will only use the approved, secure e-mail systems for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Headteacher or ICT Subject Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full via our publications scheme on request.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..(printed)

Job title . . . . . .

Appendix 3

Incident Reporting Log

Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident? Child/young person ☐ Name of child..... Staff member/ volunteer ☐ Name of staff member/ volunteer..... Other ☐ please specify.....		
Description of incident (including IP addresses, relevant user names, devices and programmes used)		
Action taken: ☐ Incident reported to head teacher/senior manager ☐ Advice sought from Safeguarding and Social Care ☐ Referral made to Safeguarding and Social Care ☐ Incident reported to police ☐ Incident reported to Internet Watch Foundation ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ E-safety policy to be reviewed/amended ☐Other (please specify)		
Outcome of investigation:		