

Mickleton Primary School

Online Safety Policy

Date of last Review: May 2019

Date of Next Review: by September 2019

Please read this policy alongside our school Safeguarding Policy and other relevant policies such as Acceptable Use Policy.

Introduction

The school believes that pupils, staff, volunteers and visitors to the school should be able to use the internet and related technologies appropriately and safely. The benefits of access to the knowledge and information available through these mediums far outweigh the risks, however, an obligation exists to ensure a duty of care is exercised and pupils are provided with a safe learning environment.
This policy, together with the related safeguarding policy, ensures statutory obligations to protect children from potential harm are met and balanced against the benefits to be gained from the use of internet-connected digital technologies to support and accelerate teaching methods and prepare pupils for life outside of the school environment.

Online safeguarding, known as e-safety is an area that is constantly evolving. We use technology and the internet extensively across all areas of the curriculum and have done all that is possible to ensure children are protected.

Purpose and Aims

The primary purpose of this policy is two-fold:

- 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 foresee ability of harm to the student or liability to the school.

This policy, along with the Acceptable Use Policy, is available for anybody to read on the school website as well as being accessible to all staff on the school shared network. This Online Safety policy is closely linked to the school Acceptable Use Policy which is read annually by both staff and pupils.

Roles and Responsibilities

Pupils

The boundaries of use of IT equipment and services in this school are given in the Pupils' Acceptable Use Policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with the Behaviour Policy.
Online Safety is embedded into our curriculum through lessons, assemblies, discussion and special events; students will be given the appropriate advice and guidance by staff. Similarly all children will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents

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 parent workshops, the school website and newsletters the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered. It is recommended that parents use the internet at home with their child, develop a similar set of rules and invest in appropriate security software.
Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will read and understand the Pupils' Acceptable Use Policy which is available on the school website. They are also able to restrict the use of images of their children by filling in a form available in the office.

Staff

Staff are to ensure that:

- Any online safety incident or potential online safety incident is reported to the Computing subject leader or to the Headteacher.
- Any disclosure by a pupil involving the internet or IT devices at home is passed to the Headteacher.
- The stand-alone Staff Acceptable User Policy should be read annually by all staff.
- They evaluate all web sites in advance of classroom use.
- They embed internet safety messages within the curriculum.
- They attend training where needed to safeguard themselves and deliver the online safety programme effectively.
- They follow the Staff AUP.
- They do not store data or images of pupils on personal digital equipment.
- Stored data and images on school computers are deleted when no longer required.
- E-mail addresses must be protected by a secure password.
- Ensure pupils' full names are not used for image labels, file names or tags.
- Mobile storage devices (memory sticks etc) are virus checked before opening any files.
- Any technical problems are reported to the Computing subject leader, who liaises with the IT technician.
- They are professional in their own internet use within and outside of school.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our school. The day-to-day management of this will be the responsibility of the Headteacher, Designated Safeguarding Lead and Computing Subject Leader.

He/she will ensure that:

- Online Safety training and relevant developments are planned and up to date and appropriate to the recipient, i.e. pupils, all staff, governing body and parents.
- The Computing subject leader has had appropriate CPD in order to undertake the day to day duties and that they support him/her in creating an internet safety culture within school.
- All online safety incidents are dealt with promptly and appropriately.
- SWGfL are informed if pupils or staff access inappropriate information accidentally and inform the LA or the police if anyone deliberately accesses inappropriate information through the internet.
- Appropriate sanctions are enforced for deliberate or careless breaches of this policy.
- The governing body is informed of the issues and the policies.

Governors

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

- Review this policy annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- The Curriculum Committee will:
  -keep up to date with emerging risks and threats through technology use
  -receive regular updates from the Headteacher/Computing Lead with regards to training, identified risks and any incidents
  -establish the effectiveness (or not) of online safety training and awareness in the school
  to recommend further initiatives for online safety training and awareness at the school
  -agree with the Headteacher, a set of appropriate sanctions for possible breaches of the Staff AUP.

Computing Subject Leader

The subject leader will:

- Establish and maintain a school-wide Computing Curriculum which embeds internet safety within each year group from Y1-Y6 including assessment of pupils' understanding of safety issues
- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy annually and bring any matters to the attention of the Headteacher.
- Work closely with the Headteacher and relevant governor on all online 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.
- Ensure any technical online safety measures in school (e.g. internet filtering, anti-virus software, firewall technology) are fit for purpose through liaison with the local authority and/or IT Technical Support.
- Ensure that staff computers and additional hardware (e.g. memory sticks) are secure through liaison with the IT technician

IT Technician

The IT technician is 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.
- Passwords are applied correctly to all adult users – in-house.
- Endure that the IT System Administrator password is secure.

Monitoring

SWGfL monitor and audit internet use to see if users are complying with the policy. Any potential misuse identified by SWGfL will be reported to the school. They will ensure:

- 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 Headteacher.

N.B. Necessary access to any site deemed 'inappropriate' for educational use should be recorded in your planning.

Incidents which appear to involve deliberate access to web sites, newsgroups and online groups that contain the following material will be reported to the police:

- Sexual images of children, apparently under 16 years old.
- Material that breaches the Obscene Publications Act in the UK.
- Criminally racist material.

If inappropriate material is accessed **accidentally**, users should immediately report this to the SWGfL at http://www.swgfl.org.uk/Staying-Safe via the Business Manager or I.T. Engineer.

Staff Computing Acceptable Use Policy

1. All staff must use the school's ICT systems and IT hardware in a responsible way, whether in school or at home
2. Whilst any IT hardware should only be used for purposes relating to employment at Mickleton Primary School, reasonable personal use during staff breaks is acceptable
3. Personal devices which have the ability to photograph or record MUST NOT be used in school
4. Staff must ensure that their use of equipment is responsible, recognising the value of using ICT to aid learning for pupils
5. The School will educate staff and pupils in the safe use of ICT and staff must embed e-safety in the pupils day-to-day work
6. For professional and personal safety, the school may monitor my use of equipment both in and out of school
7. Usernames or passwords must not be shared or disclosed, any disclosures must be reported to the Computing Subject Lead
8. Any illegal, inappropriate or harmful material or incidents must be reported immediately to the Headteacher
9. Staff must not open any attachments to emails unless the source is known and trusted
10. All data must be regularly backed up, in accordance with the school's policies
11. Staff must not try to upload, download or access any materials which are illegal, inappropriate, or may cause harm or distress to others and may not use any programmes or software which bypass the filtering/security systems in place to prevent access to such materials
12. Large capacity files may not be downloaded or uploaded without permission
13. Programmes of any type on a machine, stored programmes, or altered computer settings must be sanctioned by the school's Computing Subject Lead / IT Technician
14. Any damage or faults to school equipment must be reported to the School Business Manager
15. All school data must be kept private and confidential
16. All communication must be professional
    - No copying, removing or altering any other user's files without their permission.
    - Communicate with others in a professional manner.
    - Ensure photos are only taken and/or published when parents have given their permission to do so, and in accordance with the school's policy on the use of digital/video images.
    - Personal equipment MUST NOT be used to record images.
    - Ensure that correct permissions are held to use the original work of others.
    - No downloading or distributing copies of copyright-protected work.

Social Media

1. Staff must ensure that robust privacy settings are in place on any social media
2. Staff must not 'post' anything on social media which they would not share with pupils and parents in their day-to-day life
3. All communication with pupils/parents/carers should only be made on the official school systems and in a professional manner, not on social media
4. Staff should not discuss or comment on any school business or procedures on social media or enter into discussion with others regarding the school.

Failure to comply with this policy may result disciplinary action.

Pupil Computing Acceptable Use Policy

Mickleton Primary School is committed to safeguarding and promoting the welfare of children and young people.

Using technology to communicate has lots of advantages but there are risks. These rules will help protect you at home and school from those risks. **Remember: you won't be punished for accidentally opening inappropriate web sites.**

Pupils must:

- report to their **parents, carers or trusted adult** anything that upsets them or seems 'wrong'
- report to a **trusted adult** if they are contacted by strangers
- report to a **trusted adult** if they are bullied in any way
- report immediately to a member of staff if any of these things happen in school

Pupils must not:

- access internet sites other than those approved by a trusted adult 👎
- bring mobile phones or cameras into the classroom without permission 👎
- plug any device into a computer unless approved and virus checked before use 👎
- reveal their passwords to anyone 👎
- try to access other people's work ☹
- download music, films, games or software of any sort ☹
- sign up to any web site service without permission from a **trusted adult** ☹
- reveal or publish personal details about themselves or others on the web ☹
- send inappropriate photographs and videos by phone or online ☹
- make comments that upset other people on phones, email, messaging services or web sites ☹
- contact people not approved by a **trusted adult** ☹
- arrange to meet anyone not approved by a **trusted adult** ☹
- send hateful messages or images ☠

Sanctions

Accidental incidents will result in advice being given by the teacher to prevent any future incidents.

Deliberate minor incidents in school will lead to a warning from your phase leader. See 👎

Serious incidents (or repeated minor incidents) will mean your parents are contacted and our school behaviour policy is followed. See ☹

Illegal behaviour by anyone will be dealt with by the police. See ☠

Year 1: Signed: _____ Date: _____
Year 2: Signed: _____ Date: _____
Year 3: Signed: _____ Date: _____
Year 4: Signed: _____ Date: _____
Year 5: Signed: _____ Date: _____
Year 6: Signed: _____ Date: _____