ONLINE SAFETY POLICY

Signed by:

Mrs N Hall	Headteacher	January 2023
Mr D Hall	Chair of Governors	January 2023

Next review: Janaury 2024

Mulbarton Primary School Online Safety Policy

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.
- The school has identified a member of staff, Dominic Clarke, who has an overview of Online Safety.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation is be reviewed annually
- The Online Safety Policy was discussed by staff on 8th December 2022
- The Online Safety Policy is referred to in class discussions with children
- The Online Safety Policy was revised January 2023
- It was approved by the Governors January 2023
- Date of next review: January 2024

Contents

Rationale

The purpose of this policy is to:

- Set out the school offer with regard to the education of children, staff and the wider community in online safety.
- Set out the key principles expected of all members of the school community at Mulbarton Primary School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Ensure all staff have read and understood the Staff Code of Conduct (Guidance for safer working practice for those working with children and young people in education settings)
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to illegal, inappropriate or harmful material. For example, pornography, fake news, racist or radical and extremist views

Contact

- subjection to harmful online interaction with other users. For example, commercial advertising and adults posing as children or young adults

Conduct

- personal online behaviour that increases the likelihood of, or causes harm. For example, making, sending and receiving explicit images or online bullying

Commerce

- Financial risks, e.g. online gambling, inappropriate advertising, phishing and scams

Scope

This policy applies to all members of the Mulbarton Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors or community users) who have access to and are users of Mulbarton Primary School technologies, both in and out of Mulbarton Primary School.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website. Policy to be part of school induction pack for new staff, including information and guidance where appropriate
- Regular updates and training on online safety for all staff, including any revisions to the policy
- Acceptable User Agreement will be discussed with staff and pupils at the start of each year. Acceptable Use Agreement to be issued to whole school community on entry to the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE).

- The Online Safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school Online Safety policy will be disseminated to all members of staff and pupils

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme, based on the 'Project Evolve' rationale, which has the status of a separate subject and is planned and delivered discreetly, but is also frequently referred to in the PSHE and computing curriculum
- will remind students about their responsibilities through the pupil Acceptable Use agreement
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills and copyright

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use agreement

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- provides induction for parents which includes online safety
- runs a rolling programme of online safety advice, guidance and training for parents
- parents/carers are issued with up to date guidance on an annual basis

3. Incident management

In this school, there is:

- strict monitoring and application of the online safety policy, including the Acceptable Use agreement and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place through the CPOMS system and contributes to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

4. Managing IT and Communication System

Internet access, security and filtering

In this school:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision
- our system is managed by Sait Education who ensure that the school networks are kept secure and protected from internal and external threats
- Sait Education also ensure only authorized hardware and software are used in the school

E-mail

This school

- provides staff with an email account for their professional use and makes clear personal email should be through a separate account
- will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- will ensure that email accounts are maintained and up to date

Pupils email:

- we use school provisioned pupil email accounts that can be audited
- pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff email:

- staff will use school provisioned e-mail systems for professional purposes
- access in school to external personal e-mail accounts may be blocked
- staff will never use e-mail to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption
- communication with parents via e-mail will happen, for the most part, through the school office or via SLT. Pupil Asset can also be used by staff to send email and text messages directly to parents, who can then reply via the school office

School website

- the school web site complies with statutory DfE requirements
- most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Social networking

Staff, Volunteers and Contractors

- staff are instructed to always keep professional and private communication separate

- teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- the use of any school approved social networking will adhere to Acceptable Use Agreement

Pupils:

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- students are required to sign and follow our pupil Acceptable Use agreement

.

Parents/Carers:

- parents/carers are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

5. Data Security

Management Information System access and data transfer

- We will use guidance from the Information Commissioner's Office to ensure that we comply with the responsibilities to information rights in school
- We follow GDPR guidance and policies

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- Please use guidance from The Education Network (NEN) around Bring Your Own Device

Digital images and video

In this school:

- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement from when their child joins the school
- we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- staff sign the school's Acceptable Use agreement and this includes a clause on the use of personal mobile phones/personal equipment
- if specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for its long term, high-profile use