Swanton Morley VC
Primary School

Date agreed	June 2019
Review date	July 2020
Signed	R Robinson

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 will identify a member of staff who has an overview of Online Safety, this would usually be the Designated Safeguarding Lead (DSL).
- 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, will be reviewed annually.

Contents

1) Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Swanton Morley VC Primary School with respect to the use of technologies.
- Safeguard and protect the children and staff. Assist school staff working with children in order 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 [noting that these need to be cross referenced with other school policies].
- 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.
- 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 inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

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

Communication

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

- Policy to be available on the school website, in the staffroom and classrooms
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy
- Code of Conduct (AUP) is discussed with staff and pupils at the start of each year and is made available to the whole school community.

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, Computing policy).

- 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 as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- will remind students about their responsibilities through the pupil ICT Code of Conduct/ Acceptable Use Agreement(s);
- 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, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

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 ICT Code of Conduct/ Acceptable Use Agreements

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- offers 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 ICT Code of Conduct/AUP 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 and contribute 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 Systems

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.
- senior school managers and governors ensure the school's e-security is sufficiently maintained
- there is effective web filtering software and internet security in place
- we maintain inventories of all hardware and software used in school that also describe how these are to be configured, reviewed and kept up to date.
- appropriate technical measures are in place to protect the network including firewalls, filtering for malicious as well as inappropriate content and antivirus and malware checking.
- We ensure user privileges (for teaching staff, administrative staff and pupils) are set appropriately so all users can access the facilities they require while minimising the potential for deliberate or accidental misuse of the network.
- all users, staff and pupils, understand their e-security obligations and responsibilities through appropriate education and training including being familiar with the AUP.
- processes are in place to log, report on and monitor any e-security incidents ensuring that any damage is minimised and that lessons can be learned to prevent similar incidents from reoccurring in future.
- technical protections are in place to detect and prevent any malicious code or content which could damage the confidentiality, integrity and availability of the network.
- effective network monitoring: takes place to ensure attacks and other e-security incidents are detected quickly, allowing a rapid and effective response.
- strategies are in place to control the use of removable media (USB flash drives, portable HDDs etc.).

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
- We use anonymous e-mail addresses, for example head@, office@
- 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 LA or school provisioned e-mail systems for professional purposes
- Never use email 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.

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.

Cloud Environments

- The school's cloud service provider is maintained through the local authority who guarantee technical and organisational security.
- Pupils are taught about the online safety and 'netiquette' of storing and sharing data in the cloud both at school and at home.

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 policy, ICT Code of Conduct and AUP.

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 [age appropriate] pupil ICT Code of Conduct and AUP.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct and additional communications given when required.

5) Data Security

Management Information System access and data transfer

The school complies with the guidance from the Information Commissioner's Office ensuring that we are in compliance with the data protection act and to information rights in school.

6) Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

Pupils will only be permitted to bring their own device in to school if it is deemed beneficial to the curriculum by their class teacher. This will only happen after consultation with the Headteacher.

Bring Your Own Device (BYOD) is an addition to the curriculum and is not a compulsory element of a student's education. It is not the schools responsibility to provide or support personal student devices. The purchase, maintenance, safety, insurance and security of all personal devices must be borne by the parents/students.

School recognises the benefits to learning from offering students the opportunity to use personal devices in school to support learners and their learning. It is the intention of this policy to facilitate and support the use of personal devices in school in furtherance of individualised student learning. Students are expected to use personal devices in accordance with this policy and by using any such device in school students agree to be bound by the additional school rules and requirements set out in this policy.

- The use of personal devices falls under the school's internet AUP which all students must agree to, and comply with.
- The purpose of the use of personal devices at school is exclusively educational. Personal use of devices should not take place anywhere in school.
- Students are not permitted to connect to any external wireless or networking service (e.g. 3G/GPRS Etc.) while using a personal ICT device in school.

Rules for Acceptable Use of Personal Devices

- There are no secure facilities provided at school to store personal devices. Students therefore keep their personal device with them at all times.
- The use of a personal device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt class or Private Study areas in any way. Playing games, accessing social networks or other non-school academic related activities are not permitted.
- Students shall not distribute pictures, video or any other material relating to students or staff. (Distribution can be as small as emailing/texting to one other person or as large as posting image or video online.) Devices in this instance refer to web enabled Smartphones and Tablet devices.
- Students must check their personal device daily to ensure the device is charged, free from unsuitable material and free from viruses etc. before bringing the device into school.
- Students must check their personal device daily for basic Health and Safety compliance to ensure it is free from defects. Any personal device that has obvious Health and Safety defects should not be brought into school.
- Under no circumstances are students permitted to bring into school or use privately owned chargers for personal devices. The ONLY authorised charging facilities are any communal ones provided by school.

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 form when their daughter/son joins the school (or annually)
- 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
- Staff abide by the school's Code of Conduct/AUP and this includes the use of personal mobile phones/personal equipment