Hevingham and Marsham Primary School Partnership

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.

Contents

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Hevingham and Marsham Primary School Partnership 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 [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 (including potential radicalisation)
- 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 Hevingham and Marsham Primary School Partnership community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the schools technologies, both in and out of Hevingham and Marsham Primary School Partnership

Communication

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

- Policy to be posted on the school website/ staffroom/ 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 ' ICT 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
- Responsible Internet Use Agreement discussed with staff and pupils at the start of each year. Responsible Internet Use Agreement to be issued to whole school community, on entry to the school, and signed by parents/carers of each child, visitors to school and governors

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, Mobile Phone policy, Photography and The Use of Images 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 Responsible Internet 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, 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

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 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 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
- we have a secure, password protected Wi-fi network unavailable to unauthorised devices
- we protect the advanced settings of our networks through Administator's passwords, allowing only Norfolk Shared Services technicians sole access to these settings
- we manage our hardware and software needs through a regulated process of ICT refresh, managed by Norfolk Shared Services
- We also remove and upgrade hardware using Shared Services to guarantee any sensitive or confidential information cannot be compromised externally after removal.
- we teach each year an annually updated curriculum for age appropriate Online safety
- we have an open, specific Responsible Use policy, which sets out for adults and children the repercussions of misuse of any service or technology within school
- we have a technician fortnightly check and update our computing services and technology, in terms of quality of operation, safety of hardware, and protection against emerging threats
- we have an open and consistent policy which applies to all pupils and staff accordingly

- we employ the same procedures for an online CP incident that we would any safeguarding CP incident, thus guaranteeing our procedure is up to date and well known by all staff

- we seek new Online Safety information through the Computing Network, and take guidance from our local police force (as well as other third party Online Safety services.)

E-mail
This school

- Provides staff with an email account for their professional use, e.g. nsix.org.uk 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
- Access in school to external personal e mail accounts may be blocked
- 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

- Our school use VLE managed by ItsLearning. Each child and member of staff has a secure username and password to keep security.
- No sensitive information is uploaded onto the VLE in the staff course, and is instead saved on encrypted memory sticks.
- Some classes will upload and save work onto online cloud systems (for example Edmodo,) but again will have secure usernames, passwords and will follow the Responsible Internet Use policy

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 ICT Code of Conduct/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 Responsible Internet Use Agreement

.

Parents/Carers:

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

5. Data Security
Management Information System access and data transfer

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

6. Equipment and Digital Content
Bring Your Own Device Guidance for Staff and Pupils

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.

- The sending of abusive, offensive or inappropriate material is forbidden.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.

- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

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 materials/DVDs
- Staff sign the school's ICT Code of Conduct and are given the schools Mobile Phone policy
- If specific pupil photos (not group photos) are used on the school web site, 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