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.

- This policy should be read in conjunction with the Data Protection, Freedom of Information and Safeguarding policies

Contents

Appendices

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 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
- 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 our 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
- 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
- ICT Code of Conduct discussed between staff and pupils at the start of each year. ICT Code of Conduct to be issued to whole school community, on entry to the school and at the start of each year, to be signed by parents/carers of each child, visitors 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 ICT Code of Conduct
- 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 Codes of Conduct

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- parents are provided with an online safety newsletter monthly, which includes up to date online safety information
- runs a yearly session of online safety advice, guidance and training for parents

3. Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct 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 Administrator's passwords, allowing only NCC ICT Services 4 Education technicians access to these settings
- we manage our hardware and software needs through a regulated process of ICT refresh, managed by NCC ICT S4E
- We also remove and upgrade hardware securely using NCC ICT S4E to guarantee any sensitive or confidential information cannot be compromised externally after removal.
- We acknowledge UK Safer Internet Day annually with age appropriate sessions in all classrooms, alongside regular computing lessons where pupils learn how to use technology safely, respectfully and responsibly; as well as to recognise acceptable/unacceptable behaviour and to identify a range of ways to report concerns about content and contact.
- we have an open, specific ICT code of conduct, 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 a Managed Internet Security package which flags any threats as soon as they are detected
- we use Netsweeper Internet Filtering which is managed by NCC ICT S4E. Any changes to the filtering can only be approved by either the Head Teacher or Chair of Governors
- 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.
- Email Accounts are in line with E-Safety so that a students' gender, school, or name is not displayed
- Emails are filtered for inappropriate content. Each school has its own individual e-safety mailbox. This allows review of inappropriate emails captured by the filtering solution. A copy will automatically go into this inbox as well as the recipient's inbox

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

- Both schools use VLE managed by Its Learning. 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 ICT Code of Conduct

Social networking

Staff

- 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

Volunteers, Contractors and Governors:

- Volunteers, Contractors and Governors should not divulge any information that could lead to the identification of a member of staff or pupil
- They must not make any comments that could bring the school into disrepute

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.

Parents/Carers:

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

5. Data Security

Management Information System access and data transfer

- Please use guidance from the Information Commissioner's Office to ensure that you comply with your responsibilities to information rights in school

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 that 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

Appendix A - Pupil ICT Code of Conduct

Hevingham and Marsham Primary School Partnership
Pupil ICT Code of Conduct

The following rules apply to all pupils:

- I will only use my own login and password, which I will keep secret
- I will not look at or delete other people's files
- I will not bring disks/memory sticks/mobile phones into school without permission
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be polite and sensible
- When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know
- I will not use internet chat
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately
- I know that the school may check my computer files and may monitor the internet sites I visit
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers
- I shall learn how to stay safe on the internet
- I will log on and off in the correct way

SANCTIONS

- If I break the above rules this will result in a temporary or permanent ban on internet use
- Additional consequences may be added in line with the schools existing Behaviour Policy
- When needed, police or local authorities may have to be involved

Pupil's Agreement:

I have read and understood the school rules for Responsible Internet Use. I will follow these rules at all times when using any ICT equipment in school.

Pupil's signature……Date……

Appendix B - Staff, Governor, Visitor ICT Code of Conduct

Hevingham and Marsham Primary School Partnership Staff, Governor, Visitor ICT Code of Conduct

ICT and related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by Norfolk County Council. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with Hevingham and Marsham Primary School Partnership

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets
- All staff understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.
- All staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.
- All staff, Governors and visitors understand that they are responsible for all activities carried out under their username.
- All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Head teacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.
- All staff will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Board.
- All staff, Governors and visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.
- All staff, Governors and visitors will ensure that all data is kept secure and is used appropriately as authorized by the Head teacher or Governing Board. If in doubt they will seek clarification. This includes taking data off site.
- All staff, Governors and visitors need to be aware of the difficulties surrounding social media sites, and should not divulge any information that could lead to the identification of a member of staff or pupil, nor make comments that could bring the school into disrepute.
- Personal devices must only be used in the context of school business with explicit permission of the Headteacher.
- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- All staff will only use the approved email system(s) for any school business

- Images will only be taken, stored and used for purposes in line with school policy. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head teacher.
- All staff, Governors and visitors will comply with copyright and intellectual property rights.
- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Designated Safeguarding Lead or Head teacher in line with the school's Safeguarding Policy.

I acknowledge that I have received a copy of the ICT Code of Conduct.

Full name:……(printed)

Job title:……

Signature:……**Date:**……

Appendix C - Parent/Carer ICT Code of Conduct agreement form

Hevingham and Marsham Primary School Partnership
Parent/Carer ICT Code of Conduct

Parent / carer name:……

Pupil name: ……..

Pupil's Year Group: ……

As the parent or carer of the above pupil(s), I grant permission for my child/ren to have access to use the Internet, the Virtual Learning Environment, school email and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the ICT Code of Conduct. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy is available at http://www.hevinghamprimary.co.uk and that further advice about safe use of the Internet can be found at https://www.thinkuknow.co.uk/parents/

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, safe access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the websites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour in and out of school.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/carer signature:…… **Date:**……..