Neatishead, Salhouse & Fleggburgh Federation

Online Safety Policy

Our schools aim to be happy and safe places where everyone shares a love of learning. Our Christian core values of respect, responsibility, courage, trust, perseverance and compassion underpin all we do.

'Soar on Wings'

Norfolk County Council

Our school is the secure base from which we 'soar on wings' to realise our ambitions.

Through valuing one another and the world in which we live, we flourish.

Through providing rich opportunities, we can imagine fulfilling futures.

Through a shared love of learning, we transform lives.

Formally adopted by the Governing Board	
On:-	**18th March 2020**
Chair of Governors	**R Barker**
Date for review:-	**September 2021**

Norfolk County Council

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 Designated Safeguarding Lead (DSL) and alternate DSL will have an overview of online safety across the federation.
- 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
- The Online Safety Policy has been discussed and shared with staff.
- The Online Safety Policy is discussed with children in Circles Assembly annually.
- The Online Safety Policy was revised by the headteacher

Contents

4. Managing the IT Infrastructure
    - Internet access, security and filtering
    - E-mail
    - School website
    - Cloud Environments
    - Social networking
5. Data Security
    - Management Information System access and data transfer
6. Equipment and Digital Content
    - Bring Your Own Device Guidance for Staff and Pupils
    - Digital images and video

Guidance and Example documents (separate documents):

Legal Framework

Example Pupil ICT Code of conduct

Example Staff, Governor, Visitor ICT Code of conduct

Example Parental/Carer Permission: Use of digital images – photography and video

Example Parent/Carer ICT Code of Conduct agreement form (Feb 2016)

Guidance for schools: Parents & Carers use of photography and filming at school events

Guidance on the use of CCTV in schools including the Use of Fixed Video Cameras in the Classroom

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the federation and 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 the federation and partnership (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of technologies, both in and out of N & S.

Communication

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

- Policy to be posted on the school website and displayed in staffroom.
- 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

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 or Head of School. If the concern is about the Headteacher or Head of School, 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).

- 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 curriculum. This covers a range of skills and behaviours appropriate to their age and experience
- will remind pupils about their e safety responsibilities
- 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:

- will make 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 and newsletter and through cluster events
- runs a rolling programme of online safety advice, guidance and training for parents through the newsletter and events
- parents/carers are issued with up to date guidance via the website and newsletter

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:

1. we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision
2. the HT and Governing Body are responsible for securing best value for money.
3. Incidents are handled as per the behaviour policy and online safety policy. There is also an incident book in which reports are made to the ICT technician who visits school every two weeks to maintain the integrity of the systems in place.
4. All electronic devices' are password protected, where possible.
5. HT and administrators are the only people to have access to the main passwords for school.
6. Anti-virus- controls are installed on every PC in school.
7. An asset register is maintained in school and monitored closely by the Finance Governors.
8. All desirable and portable ICT equipment is marked.
9. Staff have ICT CPD as per individual needs identified through appraisal.
10. Pupils access ICT CPD and safety CPD is made available for parents annually.
11. The technician reviews logs and outputs and advises the HT if required.
12. Data protection policies are in place. Old data is periodically removed if no longer required.
13. E-safety monitoring is conducted by HT via email alerts. Records are maintained if action is taken as per behaviour policy. Security of school system is maintained by County

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 would 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

- We follow DfE guidance for Cloud Software Services and the Data Protection Act supported by bought in ICT Support Services

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/

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 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

- We 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

- We 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 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 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 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

****

Norfolk County Council

Appendix 1 – Computing Code of Conduct for Pupils

Appendix 2 – Computing Code of Conduct for adults working at the school

Appendix 1

This 'Code of Conduct' will be shared with pupils in Circle Assemblies. It will be displayed in all classrooms and on the school website

Computing Code of Conduct for Pupils

1. I should feel safe and enjoy being on the Internet
2. I should be able to tell someone if something has worried me on the Internet
3. I should not be bullied on the Internet, and should not bully others
4. I should help my friends stay safe on the Internet
5. I should be able to report anything that worries me on the Internet
6. I should be able to talk and play on the Internet with my friends
7. I shouldn't have to see unpleasant or hurtful things on the Internet

8. I should know how to keep my personal information safe

9. I should be able to easily search the Internet for information

10. I should learn how to stay safe on the Internet

11. I can ask an adult if I want to understand more about keeping safe on the internet

Appendix 2

Computing Code of Conduct for Staff, Governors and Visitors

Computing and the 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.

- 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 activity carried out under their username
- Staff, Governors and visitors will not install any hardware or software on any school owned device without the permission of the Headteacher
- 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 the Head teacher in line with any disciplinary

procedures. This relates to all school owned devices, including laptops provided by the school.

- All staff, Governors and visitors will only use computer technologies for uses permitted by the Head or Governing Body.
- 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 Body. If in doubt they will seek clarification. This includes taking data off site.
- 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, Governors and visitors 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 Senior Designated Professional or Head teacher in line with the school's Safeguarding Policy.
- All staff are aware of recording safeguarding incidents using the systems for reporting to the DSL
- Annual online safety training will be available to all staff

I acknowledge that I have received a copy of the ICT Code of Conduct and have read the Online Safety Policy

Full name:……(printed)

Job title:……..…

Signature:……Date:……