Online Safety Policy

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Cringleford CE VA 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
- 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)

1. Scope

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

Communication

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

- Policy to be posted on the school website and the VLE
- 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
- Through regular updates and training on online safety for all staff, including any revisions to the policy
- Staff and pupil codes of conduct discussed with staff and pupils at the start of each year. Consent forms for 'Use of digital images – photography and video' and 'Internet use and online safety' will be issued to parents when their child starts at 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 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 staff 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. 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 (Rules for responsible computer and internet use)
- 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
- provides, as part of the induction process, all staff [including regular volunteers, those on university/college placements and work experience] with information and guidance on the Online Safety Policy and the school's Staff ICT Code of Conduct

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website and through newsletters
- provides information sessions for parents which includes online safety

3. Incident management

In this school:

- 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 use the Education Network's school e-security checklist which sets out 20 e-security controls that, if implemented effectively, will help to ensure that the school network is kept secure and protected from internal and external threats.

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 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
- Email will not be used 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 website complies with statutory DfE requirements
- Most material is the school's own work; where the work of others 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 e.g. VLE.
- The use of the VLE will adhere to the Staff ICT Code of Conduct
- Staff, governors and volunteers have to sign to indicate they will follow the school's Social Media policy

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- At the start of each school year pupils will be reminded about the ICT Code of Conduct, as well as at other times during the year.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through the information and consent forms for 'Use of digital images – photography and video' and 'Internet use and online safety' and additional communications materials when required.

5. Data Security

Management Information System access and data transfer

- The school will use guidance from the Information Commissioner's Office to ensure that it complies with its responsibilities to information rights in school

6. Equipment and Digital Content

- The school will use guidance from The Education Network (NEN) around Bring Your Own Device if staff or pupils are requested to bring in their own devices

7. Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child when their child joins the school
- Parents are required to complete a consent form for 'Internet use and online safety' 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 ICT Code of Conduct and this includes a clause on the use of personal mobile phones / personal equipment

8. Use of CCTV

In this school:

- In accordance with the Data Protection Act, the school's CCTV is registered with the Information Commissioner's Office.
- The school's registration can be found by looking it up on the Information Commissioner's public register of data controllers, which can be found at

  http://www.ico.gov.uk/ESDWebPages/search.asp

or by going to

http://www.ico.gov.uk/ and following the links under “tools and resources”.

- The purpose of having CCTV is for maintaining security of the school premises.
- The school’s site manager is the designated contact in relation to the CCTV system and is the system “owner”. He is responsible for the use of the system, liaison with any security companies who operate or maintain the system, or a point of contact for anyone with concerns or queries regarding its use or wishing to gain access to the footage such as the public or police. The site manager is responsible for making sure that any data is only accessed by those with a genuine need to do so.
- There are signs in place in and around the school informing parents that CCTV is in operation, detailing a contact name and number for any enquiries relating to the school’s use of CCTV.
- The site manager has responsibility for regularly checking the quality of images being collected and also checking whether date and time stamping is accurate.

Retention of images

- Images should only be retained for as long as they are needed to achieve the purpose of maintaining school security, after which they should be destroyed. For the prevention and detection of crime, 5 working days should be sufficient as a period of time for retention of images, unless the images are required for evidential purposes, in which case they should be securely held until no longer required.

Destruction

- The site manager is responsible for destroying images. The destruction will be documented and to be done to such an extent that it renders the images irretrievable.

Access

- Access to images recorded should be limited to those required to achieve the stated, legitimate purposes. The site manager and the Senior Leadership Team will have access to view images collected. Images will only be shared with agencies such as the police. All requests for accessing images should be made in writing and the site manager and Senior Leadership Team should approve the release of information.
- Images will only be viewed in the site manager’s office so that images cannot be accidentally viewed by others.

Data subject rights

- In order to handle any requests for access to recorded footage, the school would require the following:
    - Name and role of person
    - Reason for request
    - Clear purpose for access
- Anybody granted access should view the recording within the school. A copy of the recording should not be released, unless for purposes such as prevention or detection of crime.

Additional documents attached:

Consent form for ‘Use of digital images – photography and video’

Consent form for ‘Internet use and online safety’

Staff, Governor, Visitor ICT Code of conduct

Pupil ICT Code of conduct