Norfolk County Council

Rollesby Primary and Nursery School
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.

- 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 was discussed by Staff in April 2018

- The Online Safety Policy was revised by: Elizabeth Wiggett

- It was approved by the Governors on: 25th June 2018

- Date of next review: Summer 2019

Norfolk County Council

Contents

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Rollesby Primary and Nursery 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 [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 school's 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 Rollesby Primary and Nursery School.

Communication

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

- Policy to be posted on the school website, the staff room and available to view at the school office.
- 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 with 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.

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 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 staff and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online safety can be delegated.

The Online Safety Leader (Liz Wiggett) will have, (working with the designated Child Protection Lead),an overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

An Online Safety working group will work to implement and monitor the online safety policy.

Governors

- Approve and review the effectiveness of the online safety Policy
- Appoint a governor (Emma Tacon) to act as an online safety link with the Online Safety Leader and reporting back to the governors

Head Teacher

- Ensure that all staff receives suitable CPD to carry out their online safety roles
- Create a culture where staff and learners feel able to report incidents
- Ensure that there is a system in place for monitoring online safety
- Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil
- Ensure that the school infrastructure/network is as safe and secure as possible
- Ensure that policies and procedures approved within this policy are implemented

Online Safety Leader

- Lead the online safety working group
- Log, manage and inform others of online safety incidents
- Lead the establishment and review of online safety policies and documents
- Ensure all staff are aware of the procedures outlined in policies relating to online safety
- Provide or organise training and advice for staff
- Keep up today with online safety developments
- Meet with Online Safety Governor to regularly discuss incidents and developments

Teaching and support staff

- Participate in any training and awareness raising sessions
- Read, understand and sign the Staff Code of Conduct
- Act in accordance with the Code of Conduct and Online Safety Policy
- Report any suspected misuse or problems to the Online Safety Leader or DSL
- Monitor ICT activity in lessons, extracurricular and extended school activities

Pupils

- Read, understand and sign the Pupil Code of Conduct and the agreed class internet rules
- Participate in online safety activities, follow the Code of Conduct and report any suspected misuse
- Understand that the online safety policy covers actions out of school that are related to their membership of the school

Parents and Carers

- Read and sign the Parental ICT Agreement
- Discuss online safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet
- Keep up to date with issues through newsletters and other opportunities
- Inform the Headteacher of any online safety issues that relate to the school

Technical Support Provider

- Ensure the school's ICT infrastructure is as secure as possible
- Ensure users may only access the school network through an enforced password protection policy for those who access children's data
- Maintain and inform the Senior Leadership Team of issues relating to filtering
- Keep up to date with online safety technical information and update others as relevant
- Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Leader for investigation
- Ensure monitoring systems are implemented and updated
- Ensure all security updates are applied (including anti-virus and Windows)

Community Users

- Read and agree to and follow the Staff/Visitor Code of Conduct before being provided with access to school systems

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum through discrete lessons are and across the curriculum, for all children in all years, and is regularly revisited. 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

- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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 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
- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772.

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website and via its Facebook page
- 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 and a differentiated, 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

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.
  - Parent and carers of pupils will be informed.
  - The police will be contacted if a criminal offence is suspected.

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 the minimum requirements for filtered broadband provision.
- We regularly review the safety and security of the school ICT systems.
- We have appropriate security measures in place to protect the server, firewall, routers, wireless systems and work stations from accidental or malicious attempts which might threaten the security of the schools systems and data.
- Access to the school network and internet is controlled with regard to users having clearly defined access rights to school ICT systems.

Norfolk County Council

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@
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- 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
- Ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content.
- 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 Norfolk Cloud Portal is used to access Google Tools for education. Staff and pupils can only use their LA provisioned email addresses to access the portal.

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 [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

- We comply with the responsibilities that need to be met in relation to information rights in schools, as stated in the Data Protection Policy.

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- We do not allow pupils to bring their own devices to school. Any devices/mobile phones brought to school will be left in the school office for the duration of the school day.

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 forms when their daughter/son joins the school.
  - We gain parental/carer permission for use of digital photographs or video involving their child on our school Facebook page when their daughter/son 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
- 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