



# Online Safety Policy

## Policy Consultation & Review

This policy is available on request from the school office. We also inform parents and carers about this policy when their children join our school and through our school newsletter.

This policy will be reviewed in full by the Governing Body every year. This policy was last reviewed and agreed by the Governing Body in January 2021. It is due for review on January 2022.

Signature:

Headteacher:

Date:

Signature

Chair of Governors:

Date:

## **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 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.
- The Online Safety Policy and its implementation will be reviewed bi-annually
- The Online Safety Policy was discussed by Staff on: 6/1/21

## **Contents**

### 1. Introduction and Overview

- Rationale and Scope
- How the policy is communicated to staff/pupils/community
- Handling concerns
- Reviewing and Monitoring
- GDPR compliance

### 2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent/Carer awareness and training

### 3. Incident Management

### 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

### **Rationale**

#### **The purpose of this policy is to:**

- Set out the key principles expected of all members of the school community at Reedham Primary School and Nursery 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 Reedham Primary School and Nursery 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 Reedham Primary School and Nursery.

The practical aspects of this policy implementation are contained under the School's E-Safety policy.

#### **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 '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/AUP 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 is referenced within other school policies as appropriate

- 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.

### **Compliance to General Data Protection Regulations**

Any usage of online facilities at the school must be in keeping with the school's GDPR policy.

## **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 Staff's active guidance during usage of school ICT resources in line with the pupil's ICT Code of Conduct/ Acceptable Use Agreement(s)

- 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/ Acceptable Use Agreements

### **Parent/Carer awareness and training**

This school provides information for parents/carers for online safety on the school website through the E-safety policy.

### **3. Incident management**

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct/AUP
- 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

### **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 wherever possible, 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:

- This school provides children with their own email account for educational use, e.g. @nsix.org.uk
- Staff are able to monitor and audit the use of these accounts
- 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.

**For further information on our communications please see the Communication Policy, which sets out strategies and procedures to communicate using emails and Pupil Asset messaging.**

## **Online Learning**

- The school uses G Suite Apps (Google Classroom, Gmail, Calendar, Google Meet) to facilitate its online learning. These apps are linked to the pupil and teachers' school emails.
- Children and staff will only use these emails to access the platform.
- Children's parents will not be permitted access to these platforms using their personal emails.
- Content of G Classroom is monitored by teaching staff and reported to the head teacher.
- The safe use of these Apps is taught as part of the Computing curriculum.
- Online educational content is in line with our Teaching and Learning, Feedback and Marking and AFL Policies.
- Children are taught 'netiquette' of how to use Google Meet and these are monitored closely for safeguarding issues.
- Teachers are not permitted to host Meets as a 'lone worker' as part of our Lone Worker Policy. Another member of staff will be present during Meets at all times.

## **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 school does provide access to learning materials and programmes online, e.g. G suite, Discovery Education, Maths Whizz, Nessy Learning
- Pupils are provided with their own sign in credentials
- Such access is only granted to such materials if the provider has validated security declarations in place on the safety of data

## **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
- The school has a Facebook page, which is closely monitored. Posts from parents who can only be invited to join as Reedham friends are approved and published by members of our staff.

#### **Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work, as part of their PSHE curriculum and their Computing Curriculum.

#### **Parents/Carers:**

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

### **5. Data Security**

#### **Management Information System access and data transfer**

- The school holds and processes data in accordance with its GDPR Policy and E-Data Security Policy.
- All users of the school's IT infrastructure are expected to comply with these relevant policies whether this is on school equipment or on personal/BYOD devices.

### **6. Equipment and Digital Content**

#### **Bring Your Own Device (BYOD) Guidance for Staff and Pupils**

- This school does not allow pupils to BYOD access to school networks
- Any BYOD usage by staff will require adherence to the school's ICT Code of Conduct/Acceptable Usage Policy
- Such usage will be made whilst considering the guidance given by [The Education Network \(NEN\) around Bring Your Own Device: http://www.nen.gov.uk/advice/using-consumer-it-devices-in-schools-options-opportunities-and-issues](http://www.nen.gov.uk/advice/using-consumer-it-devices-in-schools-options-opportunities-and-issues)

## **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. See 'Photography and Videos at School' Policy
- 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/AUP 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