**Caister Infant, Nursery School and Children's Centre Online Safety Policy**

**THIS DOCUMENT IS** a statement of the aims, principles and strategies for online safety at Caister Infant, Nursery School and Children's Centre.

**IT WAS DEVELOPED** through a process of consultation with teaching staff and governors.

**THIS POLICY WILL** be reviewed on a regular basis.

*Person Responsible:* **Mrs Stone**

**Rights Respecting Schools**

Caister Infant and Nursery School is currently working towards the UNICEF Rights Respecting School Bronze award.

Opportunities to teach children about the United Nations Charter for the Rights of the Child will be sought wherever possible.

**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 annually.
- The Online Safety Policy was discussed by Staff on: 22.5.2018
- The Online Safety Policy was revised by: Mrs Katie Stone
- It was approved by the Governors on:
- Date of next review: May 2019

**Contents**

**Rationale**

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

- Set out the key principles expected of all members of the school community at Caister Infant, Nursery School and Children's Centre 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 Caister Infant, Nursery School and Children's Centre community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Caister Infant, Nursery School and Children's Centre's technologies, both in and out of Caister Infant, Nursery School and Children's Centre.

**Communication**

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

- Policy to be posted on the school website and available upon request 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 is 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 is referenced within other school policies (e.g. Safeguarding and Child Protection 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 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 Code of Conduct

**Parent/Carer awareness and training**

This school:

- provides information for parents/carers for online safety on the school website
- provides parents meetings which includes online safety

**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

**E-Security**

In this school:

- we actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access. This service is provided by our IT Technician

- we actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution. This service is provided by our IT Technician

- we establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. This service is provided by our IT Technician

- we continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers

- we manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses. This service is provided by JC Comtech

- staff understand their obligations and responsibilities in relation to using their own devices in school

- we have processes and tools used to back up critical information properly with a proven methodology for timely recovery

- uses the expertise of an IT Technician provided by JC Comtech to be kept up to date with e-security risks; disseminate this information to staff when appropriate; actively manage the security configuration of network infrastructure devices (including managing passwords) and ensures and maintains the e-security of our school

- we ensure all staff and pupils are aware of their responsibilities and obligations in relation to sensitive and personal data, particularly in the light of schools' roles as data controllers under The Data Protection Act 2018

- staff are aware of the new GDPR (May 2018) and comply with data security protocol e.g. passcodes on iPods/staff iPads, locking computers when away and using school 'OneDrive' accounts to store and share information

**E-mail**

**This school**

- Provides staff with an email account for their professional use, e.g. @caisterinfant.org.uk and makes clear personal email should be through a separate account.
- We use some 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.

**Staff email:**

- Staff will use 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 website 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.

**Social networking**

**Staff, Volunteers and Contractors**

- Staff are instructed to always keep professional and private communication separate.
- Caister Infant School, Nursery and Children's Centre has a Social Network Code of Conduct that all staff are expected to read and adhere to.
- 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.
- Caister Infant, Nursery School and Children's Centre hold their own 'Facebook' social networking page for the purpose of sharing information with Parents and Carers.
- 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 taught the risks involved in social networking and how to safely report any concerns they may have about themselves or others.

**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**

- Caister Infant, Nursery School and Children's Centre uses companies, products and software that comply with our responsibilities to information rights in school.

**6. Equipment and Digital Content**

- Staff have access to digital equipment provided and supported by the School (staff iPad, iPod, laptop and Office 365 accounts that include data storage/sharing facilities and email) at all times.

**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 admission form when their daughter/son joins the school. Permission to use pupil images on Tapestry is gained in the admission form
- 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

***Safeguarding***

The school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.