Online Safety Policy

September 2023

Writing and reviewing the Online 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.

- The Designated Safeguarding Lead (DSL) has an overview of Online Safety.
- Our Online 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 Policy and its implementation will be reviewed annually
- The Online Policy was discussed by staff in September 2023.
- It was approved by the Governors September 2023.

Date of next review: September 2024

Contents

Guidance and Example documents (separate documents):

Pupil Online Code of conduct

Staff Acceptable Use policy

Staff Electronic Devices policy

Data Privacy notice: Use of digital images – photography and video

Parent/Carer Home/School agreement which includes online safety

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Falcon Junior School with respect to the use of technologies.
- Safeguard and protect the children, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Have clear structures to deal with online abuse.
- 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The main areas of risk for our school community can be summarised as follows:

Content

- Being exposed to illegal, inappropriate or harmful content such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact

- Being subjected to harmful online interaction with other users, such as peer -to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct

- Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Scope

This policy applies to all members of Falcon Junior 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 Falcon Junior School.

Communication

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

- Policy to be posted on the school website and given to staff.
- 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 Acceptable Use of Technology Agreement' and 'Staff Electronic Devices Policy' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy
- Pupil Online Code of Conduct is discussed annually with children.
- Online safety is included in the Home/School Agreement which the wider community sign on entry

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 policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Combat Bullying policy, 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 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 curriculum

This school:

- has a clear, progressive online safety education programme. This covers how to use technology safely, respectfully and responsibly, how to recognise acceptable and unacceptable behaviour and a range of ways to report concerns about content and contact. Children also learn that people sometimes behave differently online, including by pretending to be someone they are not
- will teach pupils how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- will ensure pupils know how information and data is shared and used online
- will remind pupils that the same principles apply to online relationships as to face-to-face relationships, through the Pupil Online 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
- will teach pupils to be critically aware of the materials they read and show them how to validate information before accepting its accuracy

Governors:

- will ensure that they have read and understand this policy
- will agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- will ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- will ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- will ensure school has appropriate filters and monitoring systems in place and regularly review their effectiveness in line with the Department for Education's filtering and monitoring standards. The appropriateness of any filtering and monitoring systems will take into consideration the risk assessment required by the Prevent Duty.

- will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- will consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs versus safeguarding risks.

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues which will make staff aware that :

-technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse not only from others but also peers

-physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

- As part of the induction process all staff (including those on university/college placement and work experience) will be provided with information and guidance on the Online Safety Policy.

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- runs a rolling programme of online safety advice, guidance and training for parents
- parents/carers are offered up to date guidance on a regular basis

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3. Incident management

In this school:

- all staff and volunteers respond appropriately to all online safety concerns including those about sexual violence and/or harassment, both online and offline and maintain an attitude of 'it could happen here'

- there is strict monitoring and application of the Online policy, including the Online Code of Conduct. The DSL will deal with any incidents in line with the school's behaviour and safeguarding policies.
- 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 and to ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- we have procedures in place to ensure that anti-virus and malware protection systems are installed and maintained on a regular basis

E-mail

This school

- provides staff with an email account for their professional use, e.g. @falcon.norfolk.sch.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 the online safety and 'netiquette' of using e-mail both in school and at home.
- Emails and website use is monitored by a member of the SMT.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- 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.
- Staff 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.
- Class Dojo is used by staff as a means of communication with parents. When using, both Class Dojo and Twitter, staff will adhere to the 'Staff Acceptable Use Agreement'

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our Online Safety curriculum work.
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- Pupils are required to follow our pupil Online Code of Conduct
- Children will only bring a mobile phone to school if they will need it for their safety on their way home. Any mobile phone brought to school will be passed to the child's class teacher for safe keeping. Children are not allowed to use personal mobile devices in school.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our Home/ School agreement and additional communications materials when required.
- The school will let parents know:
    - What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6. Data Security

Management Information System access and data transfer

- Teachers and office staff have access to the MIS (Pupil Asset)
- Please use guidance from the Information Commissioner's Office (https://ico.org.uk/for-organisations/education/) to ensure that you comply with your responsibilities to information rights in school
- Staff must log out of Pupil Asset when they are not near the computer

7. Information Security and Access Management

- The ICT technician and DSL will check the appropriate level of security protection is in place in order to safeguard systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies

8. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- Please use guidance from The Education Network (NEN) around Bring Your Own Device (http://www.nen.gov.uk/advice/bring-your-own-device-byod)

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
- 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 'Staff Acceptable Use of Technology Agreement' and this includes a section on the use of personal mobile phones/personal equipment
- If specific pupil photos (not group photos) are used on the school website, 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