Online Safety Policy

September 2021

Part of the Safeguarding Umbrella
Approved by Governing Body
Review date September 2022

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.

- 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 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 February 2019.
- It was approved by the Governors September 2021.

Date of next review: September 2022

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 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.
- 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

- 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)

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 one of the Co-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, 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

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

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. nsix.org.uk or @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 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;

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.
- Pupils are required to follow our pupil Online Code of Conduct

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our Home/ School agreement and additional communications materials when required.

5. 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

6. 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 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

Appendix-COVID-19 school closure arrangements Online Safety at Falcon Junior School. (To be used in the event of a school closure).

This section of the whole school policy was created in response to Covid19 and agreed by the Governing Body May 2020.

Context

From 20th March 2020 parents were asked to keep their children at home, wherever possible, and for schools to remain open to provide care for a limited number of children; children who are vulnerable, and children whose parents are critical to the COVID-19 response and cannot be safely cared for at home.

Learning is now taking place remotely and this appendix offers further guidance to staff, volunteers, visitors and parents on online safety. This appendix should be read in conjunction with the whole school online safety policy and not as a standalone document.

Remote Learning

At Falcon Junior School, we recognise that it is more important than ever that we provide a safe environment for pupils working online. We will continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online via our IT systems and/or recommended resources.

Staff:

- Staff will only communicate with pupils via nsix emails/logins as this ensures the filtering and monitoring software is enabled.
- Staff will use either nsix emails or Class Dojo to communicate with parents
- If ringing parents, staff will use either the school mobile or use 'caller withheld' to ensure the pupil/parent is not able to identify the staff member's personal contact details.
- Staff will maintain appropriate professional boundaries and avoid behaviours which could be misinterpreted when contacting children and parents online.
- Staff will continue to report any concerns about online safety via cpoms.
- Staff will only use Google Meet as a platform to hold class meetings.
- Staff will consider the following points when engaging in online meetings:
  -wear appropriate clothing
  -think about the background: photos, art work, identifying features, mirrors-ideally the background will be a plain wall or blurred.
  -both staff and pupils should be in living/communal areas-not in bedrooms

-avoid one to one situations- ask a parent to be in the room or ask a colleague or member of SLT to join the session
-it is the staff member's responsibility to act as a moderator; raise any issues of suitability (dress, location or behaviour) with the child and/or parent and if needbe end the online interaction.

Staff can receive professional support with any online safety issues from the UK Safer Internet Centre' professional helpline by ringing 0344 381 4772 or e-mailing helpline@saferinternet.org.uk .

Pupils:

- Pupils are required to follow the school's online code of conduct that they signed in September.
- Pupils must report any problems they have online immediately to their parent/carer and then to their class teacher via their nsix e-mail accounts.

Parents/carers:

- Parents and carers will be informed of any websites their children will be expected to access whilst completing their home learning and the school staff their children will interact with.
- Parents and carers should ensure a safe online environment. This means setting age-appropriate parental controls on digital devices and using internet filters to block malicious websites. These are usually free, but often need to be turned on.
- Parents and carers may choose to supplement the school or college online offer with support from online companies and in some cases individual tutors. If choosing to do this, parents should ensure that they are securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children.

The following websites offer valuable advice for parents:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and careers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers