# Online Safety Policy

## Introduction

Technology is an important and essential part of the learning experience at The Free School Norwich. We are committed to ensuring that our children leave with the skills and knowledge that will help them to thrive in our digital age. Tablets are used regularly in the lower school, whilst the ICT suite is used frequently during ICT lessons and for cross-curricular topics. The teachers use the internet daily with the children. It is therefore also vital that we teach children how to use this valuable resource safely. This policy understands that most children have access to iPads and computers at home and within school. It promotes the use of these technologies whilst committing to keeping our children aware of and safe from the potential risks. We will demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / guardians and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

## Aims

- To ensure that the safety and wellbeing of children and young people is paramount while they are using the internet, social media or mobile devices.
- To provide staff, volunteers, visitors and contractors with the overarching principles that guide our approach to online safety
- To ensure that, as an organisation, we operate in line with our values and to take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in The Free School Norwich's activities.

## Legislation

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying

• child protection learning.nspcc.org.uk/child-protection-system

**Responsibilities**

The Principal will be responsible for the implementation of this policy.

ICT Co-ordinator will act as E- Safety Co-ordinator and will:

- compile logs of e-safety incidents;
- report to the Principal on recorded incidents;
- ensure that staff are aware of this guidance;
- provide / arrange for staff training;
- liaise with school technical staff;
- advise on e-safety policy review and development;
- be responsible for the IT infrastructure and ensure that it is not open to misuse or malicious attack;
- ensure that users may only access the networks and devices through an enforced password protection policy and multi-factor authentication when working remotely;
- keep up to date with e-safety technical information in order to carry out their role;
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse where deemed necessary; and
- implement any agreed monitoring software / systems;
- liaise with the Principal on any investigation and action in relation to e-incidents.

Teaching and Support Staff will:

- are responsible for using school digital technology systems in accordance with the acceptable use policy;
- maintain awareness of school e-safety policies and practices whilst following the staff acceptable use policy;
- report any suspected misuse or problem to the Principal;
- ensure that all digital communications with pupils / parents / guardians / fellow staff are on a professional level and conducted on school systems;
- ensure pupils understand and follow e-safety policies;

- ensure that children are taught about relevant, age appropriate e-safety systems through teaching activities and curriculum delivery. These include but are not limited to:
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.
    a) sharing of personal data;
    b) inappropriate on-line contact with adults/ strangers
    c) potential or actual incidents of grooming; and
    d) cyberbullying
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- monitor the use of digital technologies (including mobile devices, cameras etc during school activities).

Pupils:

- are responsible for using school digital technology systems in accordance with the acceptable use policy;
- will understand and follow e-safety policies, and where appropriate, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents/ guardians:

- will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc;
- will be encouraged to support the school in the promotion of good e-safety practice; and

Parents/ carers should follow school guidelines found in this document and in our Mobile Phone and Camera policy on:

- digital and video images taken at school events;
- access to parents' sections of the school website / pupil records; and
- their children's / pupils' personal devices in the school (where this is permitted).

Community Users/ Contractors

On the rare occasions where such groups have access to school networks/ devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

**Online Safeguarding**

We believe that:

- children and young people should never experience abuse of any kind;
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges;
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online;
- we have a responsibility to help keep children and young people safe online, whether or not they are using The Free School Norwich's network and devices;
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse;
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- ensuring that all staff are aware of e-safety issues;
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults;

- supporting and encouraging the young people at The Free School Norwich to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others;
- supporting and encouraging parents and carers to do what they can to keep their children safe online;
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person;
- reviewing and updating the security of our information systems regularly;
- ensuring that usernames, logins, email accounts and passwords are used effectively and kept secure;
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate;
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given;
- providing supervision, support and training for staff and volunteers about online safety; and
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

**Online Abuse**

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse);
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation;
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account;
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

**Related policies and procedures**

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection;
- Procedures for responding to concerns about a child or young person's wellbeing;
- Dealing with allegations of abuse made against a child or young person;
- Managing allegations against staff and volunteers;
- IT Acceptable Use policy;
- Code of conduct for staff and volunteers;
- Anti-bullying policy and procedures;
- Mobile Phone and Camera policy;
- Photography and image sharing guidance.

**Principal:** Tania Sidney-Roberts
**Chair of Governors:** Andy Skeggs
**Policy Approved:** Christmas Term 2020
**Policy Review Date:** Christmas Term 2021