HACKNEY CITY FARM.CO.UK

1a Goldsmiths Row, London E2 8QA

TEL: +44 20 7729 6381

farm@hackneycityfarm.co.uk

- The School at Hackney City Farm -

Online Safety Policy

INTRODUCTION

The School at Hackney City Farm recognises the need to maintain a strategy for effective use of the internet as a valuable tool for learning.

It also recognises the need to protect users, in particular young people, from offensive and dangerous material and acknowledges the need to ensure that all users make responsible use of the internet.

RATIONALE

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at The School at Hackney City Farm with respect to the use of IT-based technologies.
- Safeguard and protect young people and staff.
- Assist school staff working with young people to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying.
- 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.

SCOPE

This policy applies to all members of The School at Hackney City Farm who have access to and are users of the school computing systems, both in and out of the school.

AREAS OF RISK

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

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Online bullying in all forms.
- Identity theft (including ‘frape’- hacking Facebook profiles) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being amount of time spent online.
- Sexting (sending and receiving of personally intimate images)
- Extremism.
- Copyright.

ROLES AND RESPONSIBILITIES

School Manager

- Take overall responsibility for online safety provision.
- Take overall responsibility for data and data security and ensure the security of the school IT system.
- Ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.
- Keep up to date with the school online safety policy and technical information. Inform and update others as relevant.
- Be aware of procedures to be followed in the event of a serious e-safety incident.
- Ensure that all electronic data held on students is adequately protected.

- Be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant.

It Tutor / (DSL)

- Investigate provision which exists for misuse detection and malicious attack e.g. keeping virus protection up to date.
- Ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
- Ensure that users may only access the school networks through an authorised and properly enforced password protection policy.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Designated Safeguarding Lead

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness and commitment to online safeguarding throughout the school community.
- Ensure that online safety education is embedded across the curriculum.
- Communicate regularly with the Manager of Hackney City Farm and the Designated Safeguarding Governor.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Ensure that an online safety incident log is kept up to date.
- Regularly update knowledge and understanding of e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
  - Sharing of personal data.
  - Access to illegal / inappropriate materials.
  - Inappropriate on-line contact with adults/strangers.
  - Potential or actual incidents of grooming.
  - Online bullying and use of social media

Designated Safeguarding Governor

- Ensure that the school follows all current online safety advice to keep the students and staff safe.
- Approve the online safety policy and review the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports.
- Support the school in encouraging parents and the wider community to become

engaged in e-safety activities.

Members of staff

- Report any online safety related issues that arise to the Designated Safeguarding Lead.
- Embed online safety issues in all aspects of the curriculum and other school activities.
- Closely supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).
- Ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- Read, understand and help promote the school e- safety policies and guidance.
- Read, understand, sign and adhere to the school staff Acceptable Use Agreement.
- Be aware of online safety issues related to the use of mobile phones, cameras and handheld devices. Monitor their use and implement current school policies with regard to these devices.
- Maintain an awareness of current online safety issues and guidance e.g. through CPD.
- Model safe, responsible and professional behaviours in their own use of technology.
- Ensure that any digital communications with students should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones.

Young People

- Read, understand, sign and adhere to the Student Acceptable Use Policy
- Have a clear understanding on how to stay safe online.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Know and understand school policy on the use of mobile phones, digital cameras and handheld devices.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

Parents / Carers

- Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school use of photographic and video images.

- Read, understand and promote the school Student Acceptable Use Agreement with their children.
- Consult with the school if they have any concerns about their children's use of technology.

COMMUNICATION

The policy will be communicated to staff and young people in the following ways:

- Policy to be posted on the school website /staff handbook/classrooms.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with students at the start of each year.
- Acceptable use agreements to be held in student and personnel files.

HANDLING COMPLAINTS

- The School will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed, or any consequences of internet access.
- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:
    - Meeting with the Head of School and parents or carers.
    - Removal of internet or computer access for a period.
    - Referral to LA/Police.
- Our Designated Safeguarding Lead acts as first point of contact for any complaint.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with child protection procedures.

REVIEW AND MONITORING

- The Online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

STUDENT ONLINE SAFETY CURRICULUM

This school has an online safety education programme as part of the curriculum.

- Develop a range of strategies to evaluate and verify information before accepting its accuracy.
- Be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be.
- Know how to narrow down or refine a search.
- Understand how search engines work and to understand that this affects the results they see at the top of the listings.
- Understand acceptable behaviour when using an online environment or email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- Understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- Understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
- Understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- Understand why they must not post pictures or videos of others without their permission.
- Know not to download any files e.g. music files without permission.
- Have strategies for dealing with receipt of inappropriate materials.
- Understand why and how some people will ‘groom’ young people for sexual reasons.
- Understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- Know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Young people will be reminded about their responsibilities through an end-user Acceptable Use Policy which they will sign.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- When copying materials from the web, staff and young people will understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Staff and the young people will understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop- ups; buying online; online gaming/gambling.

STAFF AND GOVERNOR TRAINING

We ensure that staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

We make regular training available to staff on online safety issues and the school online safety education program.

All new staff receive information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies as part of the induction process.

PARENT AWARENESS AND TRAINING

The school discusses the Acceptable Use Agreement with parents of new students to ensure that the principles of online safe behaviour are made clear.

We provide suggestions for safe Internet use at home.

PERSONAL MOBILE PHONES AND MOBILE DEVICES

- Young people are permitted to bring their mobile devices to school. However, they must not interfere with learning or distract others. It is an expectation that students are sensible with their use and follow the school guidelines.
- Mobile devices are not to be used during class time and at the lunch table, unless instructed.
- If a mobile device is used in class without permission the gate policy will be implemented for the whole class, the following lesson.
- If this arrangement is repeatedly abused, all phones will be left in the office before students gain entry to the class.
- Mobile phones brought into school are entirely at the staff member, students, parents' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed by the School Manager.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that

examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members.

STAFF USE OF PERSONAL DEVICES

- Staff will use the school phone where contact with students, parents or carers are required.
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode.
- Mobile phones or personally owned devices will not be used during teaching periods other than in emergency circumstances.

DIGITAL IMAGES AND VIDEO

- 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 students in online photographic materials or include the full names of students in the credits of any published school produced video materials/ DVDs.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work.
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.