Laburnum Boat Club
Hackney's Community Boating Project
Laburnum Street, Hackney, London E2 8BH
Telephone: 020 7729 2915
email: info@laburnumboatclub.com
www.laburnumboatclub.com

E-Safety Policy

February 2015

1. The purpose of this policy is to:

1.1. Set out the key principles expected of all members of the Laburnum Boat Club with respect to the use of ICT-based technologies.

1.2. Safeguard and protect the children and staff of Laburnum Boat Club, in accordance with the Safeguarding policies.

1.3. Assist staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

1.4. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

1.5. Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other policies.

1.6. Ensure that all members of Laburnum Boat Club are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

1.7. Minimise the risk of misplaced or malicious allegations made against adults who work with children.

2. The main areas of risk for Laburnum Boat Club can be summarised as follows:

2.1. Content

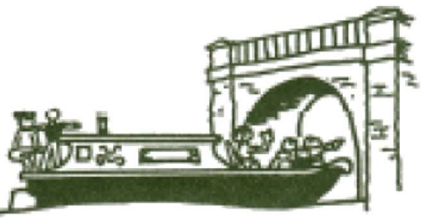
- Exposure to inappropriate content. Including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity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

2.2. Contact

- Grooming
- Cyber-Bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

2.3. Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- (Ref Ofsted 2013)



3. Scope:

3.1. This policy applies to all members of Laburnum Boat Club (including staff, members, volunteers, parents/carers, visitors, community users) who have access to and are users of Laburnum Boat Club ICT systems, both in and out of Laburnum Boat Club

3.2. The Laburnum Boat Club will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the club.

Role	Key Responsibilities
Club Coordinator	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date

E-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the club e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout Laburnum Boat Club
	• ensures that e-safety education is embedded across the curriculum
	• To communicate regularly with Senior staff and the designated e-safety committee member to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in 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
	  • cyber-bullying and use of social media

Management Committee	• To ensure that the Club follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Management Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Management Committee has taken on the role of E-Safety member • To support the club in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety member will include: • regular review with the E-Safety Co-ordinator / Officer including e-safety incident logs, filtering / change control logs)

All staff	• To read, understand and help promote the club's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current club policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Members	• Read, understand, sign and adhere to the member Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/carers	• to support the club in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the club's use of photographic and video images • to read, understand and promote the Pupil Acceptable Use Agreement with their children • to consult with the club if they have any concerns about their children's use of technology

4. Communication

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

- Policy to be posted on the website and folder.
- Policy to be part of induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.

5. Handling Complaints

5.1. The club will take all reasonable precautions to ensure e-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 club computer or mobile device. Neither the club nor Management Committee can accept liability for material accessed, or any consequences of Internet access.

5.2. Staff and members are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling E-Safety Coordinator/Club Coordinator;
- Informing parents or carers;

- Removal of Internet or computer access for a period
- Referral to Police

5.3. Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Club Coordinator.

5.4. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with child protection procedures.

6. Review and Monitoring

6.1. The e-safety policy is referenced from within other club policies: Child Protection policy, Anti-Bullying policy.

6.2. The club has an e-safety coordinator who will be responsible for document ownership, review and updates.

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

6.4. The e-safety policy has been written by the club e-safety Coordinator and is current and appropriate for its intended audience and purpose.

6.5. There is widespread ownership of the policy and it has been agreed by the senior team and approved by management committee. All amendments to the club e-safeguarding policy will be discussed in detail with all members of staff.

7. Knowledge of Technology

7.1. This club recognises that the internet and associated technologies have positive and negative aspects. While it is not the intention to 'pretend these technologies do not exist', sometimes these technologies may be appropriate and the club has a duty to allow safe usage

7.2. This covers a range of skills and behaviours appropriate to the young person's age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To 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.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; 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.

7.3. Plans Internet use carefully to ensure that it is age-appropriate.

7.4. Ensures staff will model safe and responsible behaviour in their own use of technology.

7.5. Ensures that when copying materials from the web, staff and members understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

7.6. Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

8. Equipment and Personal Devices

8.1. Mobile phones brought into club are entirely at the staff member, student's & parents' or visitors own risk. The club accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into the club

8.2. Members are strongly encouraged not to bring their phones to the club. If they must then again, they are strongly encouraged to hand them in to the coffee bar for safe keeping.

8.3. 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 otherwise by the Club Coordinator. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Club Coordinator is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

8.4. Where parents or members need to contact each other during the club time, they should do so through the club's telephone. Parents are advised not to contact their child via their mobile phone but to contact the office.

8.5. Mobile phones and personally-owned mobile devices brought in to the club are the responsibility of the device owner. The club accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

8.6. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the club site, e.g. changing rooms and toilets.

8.7. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

8.8. The Club accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

8.9. Members should protect their phone numbers by only giving them to trusted friends and family members. Members will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

8.10. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

8.11. Staff will be issued with a club phone where contact with members, parents or carers is required.

8.12. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during working time unless permission has been granted by a member of the senior leadership team in emergency circumstances.

8.13. Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

8.14. If a member of staff breaches the club policy then disciplinary action may be taken.

8.15. Where staff members are required to use a mobile phone for club duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a club mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a club-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes.

9. Digital Images and Videos

9.1. We gain parental / carer permission for use of digital photographs or video involving their child as part of the club membership form when their daughter / son joins the club.

9.2. We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published club produced video materials / DVDs.

9.3. Members 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.

9.4. Members 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 identity 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.