OYAP Trust: e-safety policy

This policy and the procedures that it underpins apply to all staff, including senior managers and the board of trustees, paid staff, volunteers and sessional workers, agency staff, students and anyone working on behalf of OYAP Trust.

The policy aims to:

- Protect children and young people who receive (name of group/organisation)'s services and who make use of information technology (such as mobile phones, games consoles and the Internet) as part of their involvement with us;
- to provide staff and volunteers with the overarching principles that guide our approach to e-safety;
- to ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

We recognise that:

- the welfare of the children/young people who come into contact with our services is paramount and should govern our approach to the use and management of electronic communications technologies;
- all children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, 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 esafety;
- the use of information technology is an essential part of all our lives; it is involved in how we as an organisation gather and store information, as well as how we communicate with each other. It is also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all. However, it can present challenges in terms of how we use it responsibly and, if misused either by an adult or a young person, can be actually or potentially harmful to them.

We will seek to promote e-safety by:

- appointing an e-safety coordinator (Helen Le Brocq – named person for Child Protection)
- developing a range of procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT;
- supporting and encouraging the young people using our service to use the opportunities offered by mobile phone technology and the internet in a way that keeps themselves safe and shows respect for others; supporting and encouraging parents and carers to do what they can to keep their children safe online and when using their mobile phones and game consoles;
- incorporating statements about safe and appropriate ICT use into the codes of conduct both for staff and volunteers and for children and young people;
- use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a child/young person (these may include breaches of filtering, illegal use, cyberbullying, or use of ICT to groom a child or to perpetrate abuse);
- informing parents and carers of incidents of concern as appropriate;
- reviewing and updating the security of our information systems regularly;
- providing adequate physical security for ICT equipment;
- ensuring that user names, logins and passwords are used effectively;

- using only official email accounts provided via the organisation, and monitoring these as necessary;
- ensuring that the personal information of staff, volunteers and service users (including service users' names) are not published on our website without express permission;
- 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;
- any social media tools used in the course of our work with children, young people and families must be risk assessed in advance by the member of staff wishing to use them;
- providing effective management for staff and volunteers on ICT issues, through supervision, support and training;
- examining and risk assessing any emerging new technologies before they are used within the organisation.
- Observe the procedure for handling personal information (see attached)

Handling personal information

Please follow the guidance below when handling personal data

- Remove any attachments (i.e. booking forms) from emails
- Print booking forms upon receipt and keep a hard copy file in the locked cupboard
- Password protect any documents containing personal information
- Do not keep for longer than necessary personal information about young people
- All incidents of security breaches must be reported to the General Manager and Director
- The Director will investigate the incident which will be recorded on the Security Notification Form.
- The Director will inform the trustee Champion for Child Protection and the chair of Trustees and report the incident with the Information Commissioners Office where appropriate.

The name of our e-safety coordinator is Helen Le Brocq
She can be contacted on 01869 602560 helen@oyap.org.uk

We are committed to reviewing our policy, procedures and good practice annually.