TILEYARD EDUCATION
EQUALITY AND DIVERSITY POLICY

Policy Owner: Tileyard Education Manager
Last Updated: February 2017
Last Reviewed: April 2019
Next Review Date: April 2020

Purpose

The Equality Act 2010 and the Equality Amendment Order 2012 require Tileyard Education and TY-e to maintain an Equality & Diversity policy to guarantee Tileyard Education and TY-e's commitment to develop an inclusive and supportive environment for students and staff where all are able to participate and where everyone has the opportunity to fulfill their potential.

This policy is to be used in conjunction with;

- Equality and Diversity Procedure.
- Disability Policy & Procedure General Principles

Within a context of respecting difference, Tileyard Education and TY-e is committed to ensuring that there is equal opportunity for all regardless of gender, age, race, disability, marital or civil partnership status, pregnancy, maternity & paternity, gender re-assignment, religion or belief or sexual orientation.

Tileyard Education and TY-e will not discriminate unfairly on the grounds of gender, age, race, disability, marital or civil partnership status, pregnancy, maternity or paternity, gender reassignment, religion or belief or sexual orientation.

Tileyard Education and TY-e is committed to removing unfair and discriminatory practices in all contexts and at all levels and, as a result, to encouraging full contribution from its diverse community. Tileyard Education and TY-e is committed to actively opposing all forms of discrimination and calls on all members of its community to make a similar personal commitment.

Tileyard Education and TY-e is committed to providing musical education and training to meet the aspirations of as many as possible of those whom it deems to have the ability and motivation to benefit.

Tileyard Education and TY-e believes that all its students, employees and visitors are entitled to be treated with dignity and, as such, that discriminatory behaviour will not be tolerated.

Equality and diversity priorities will align with and underpin Tileyard Education and TY-e Strategic Plan as well as operational planning at all levels.

Tileyard Education and TY-e will make reasonable adjustments for students and staff in accordance with identified needs wherever possible within the statutory criteria.

Scope

This policy covers all aspects of Tileyard Education and TY-e's academic provision and business process including, but not limited to, programme development, student recruitment and admissions, learning and teaching, assessment, advertisements, recruitment, induction, pay, conditions of service, staff development, change management, promotions, grievance and disciplinary procedures, course development.

This policy also applies to relationships with other institutions and with suppliers and contractors.

This policy also applies to potential students and employees.

Definitions

Discrimination

Discrimination is unequal or differential treatment which leads to one person being treated more or less favourably than others are, or would be, treated in the same or similar circumstances on the grounds of gender, age, race, disability, gender identify or re- assignment, marital or civil partnership status, pregnancy, maternity & paternity, religion or belief or sexual orientation. Discrimination may be direct or indirect.

Protected Groups

2.1 Age
2.2 Disability
2.3 Gender
2.4 Marriage and Civil Partnership
2.5 Pregnancy, Maternity & Paternity
2.6 Race
2.7 Sex
2.8 Sexual Orientation
2.9 Religion and Belief

Direct Discrimination Direct discrimination occurs when a person or a policy, criterion or practice intentionally treats a person less favourably than another on grounds related to their identity as one of the protected groups above.

Indirect Discrimination Indirect discrimination occurs when a person or a policy, criterion or practice applies equally to all but:

- is detrimental to a considerably larger proportion of people from a group identified as having one or more of the protected characteristics than from the general populace
- the need for the application of the policy cannot be justified on a neutral basis
- the person to whom the policy, criterion or practice is being applied suffers unfair detriment from the application of said policy, criterion or practice Harassment Harassment occurs when a person is subjected to unwanted conduct that has the purpose or effect of violating their dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment. The Protection from Harassment Act 1997 makes harassment a criminal offence. Victimisation Victimisation occurs when a person is treated less favourably because they have bought or intend to bring internal or legal proceedings or they have given or intend to give evidence in an internal or legal proceeding.

Discriminatory Language

As a general rule, if age, or gender, or sexual preference, or ethnicity, or any other category of identification or difference, is not relevant to a discussion, then it should not be specified. If it is relevant, then it should be discussed respectfully. The use of offensive language; derogatory terms, stereotypes, or generalisations about an individual or group will not be tolerated.

The following are some of the major forms of discriminatory language: extra-visibility, invisibility, stereotypes, derogatory labels, offensive language & trivialising language.

Conduct

Any employee, or contractor who is found (after investigation), to have acted in a manner which contravenes this policy towards students, tutors, customers or suppliers, fellow colleagues and partners of Tileyard Education will be subject to potential disciplinary procedures and action.

Responsibilities

Every member of Tileyard Education and TY-e community has a moral and legal responsibility to promote equal treatment and opportunity within that community and to respect its diversity.

Tileyard Education and TY-e expects that all students, employees and/or visitors will act in such a way as to avoid subjecting other students, employees and/or visitors to direct or indirect discrimination and/or harassment or victimisation on the grounds of their gender, age, race, disability, gender identity or re-assignment, marital or civil

partnership status, pregnancy, maternity or paternity, disability, religion or belief or sexual orientation.

The Board of Directors take responsibility for achieving the objectives of this policy and for ensuring compliance with the Equality Act 2010 and the Equality Act Amendment Order 2012.

The Tileyard Education Manager is responsible for matters relating to equality of opportunity in student recruitment and admissions, for developing policies which meet legislation and best practice, for monitoring the impact of these policies on different minority groups, and for providing relevant student recruitment and admissions statistics.

The Student and Staff Development Manager is responsible for matters relating to equality of opportunity in learning, teaching and assessment, for developing policies which meet legislation and best practice, for monitoring the impact of these policies on different minority groups, and for providing relevant student statistics.

The Tileyard Education Manager is responsible for matters relating to equality of opportunity in employment, for developing policies which meet legislation and best practice, for monitoring the impact of these policies on different minority groups, and for providing relevant employment statistics.

Students and staff are responsible for ensuring that their actions are carried out in accordance with this policy. They may be held personally to account should their actions fall short of the requirements of this policy in any way.

Implementation & Communication

The Tileyard Education Manager will be responsible for the co-ordination of policy initiatives. These initiatives will be developed in consultation with students and staff. Students and staff will be regularly informed of their responsibilities towards the promotion and implementation of relevant policies and procedures and regular training and development will be provided.

The Equality and Diversity policy is available on the VLE and Tileyard Education website.

Breach of the policy

Tileyard Education and TY-e will take seriously any instance of non-adherence to the Equality and Diversity policy by students, staff or visitors. Any instances of non-adherence will be investigated with the intent of resolving matters. Where

appropriate, such instances may be considered under the relevant disciplinary policy for staff or students.

TILEYARD EDUCATION
DATA PROTECTION POLICY AND MANUAL

Policy Owner: Tileyard Education Manager
Last Updated: February 2017
Last Reviewed: February 2017
Next Review Date: February 2018
Last reviewed: April 2019

CONTENTS 2

FOREWORD 3

DATA PROTECTION POLICY 4
Procedure 4
Data Controller 4
Data Protection Officer 5
Data Owner 5
Responsibilities of Data Subjects 5
5
Data Types 5
Processing Personal Data 6
Conditions for Processing 8
Organisational Measures 9
Rights of Data Subjects 9
Access by Data Subjects 10

EMPLOYEE RECORDS DATA PROTECTION POLICY 11
PROCEDURE 11
Monitoring 11
Benefits 11
Employee Records and Retention 12
Health Records 12

DATA SECURITY 13

FREEDOM OF INFORMATION 14

FOREWORD

This Data Protection Manual is the means by which Tileyard Music Education Ltd trading as Tileyard Education satisfies the requirements of GDPR regulations, its stakeholders with particular regard to management responsibility for Data Protection, Employee Data Protection, Management Information, Data Security and Freedom of Information.

Tileyard Education is obliged to ensure that this Data Protection Manual is fully and completely understood by its employees, and that its procedures are implemented and maintained at all times. This Data Protection Manual has been produced in accordance with the requirements of the Data Protection Act 1998 (including EU Directive 95/46/EC). All of the components of the Data Protection system shall be periodically and systematically reviewed by both internal and external Quality Audit procedures.

Tileyard Education Manager is responsible for the control of all matters relating to the implementation of this Data Protection Manual; however, data protection compliance is fundamental to all the work undertaken by Tileyard Education and, as such, all personnel at every level shall practice the procedures herein established.

DATA PROTECTION POLICY

The Data Protection Act 1998 requires Tileyard Education to maintain this Data Protection Policy, and to register as a Data Controller with the Information Commissioner's Office in order to guarantee compliance with the provisions of the Act.

Schedule 1 of the Data Protection Act 1998 sets out eight principles of Data Protection with which any party handling personal data must comply.
To this end Tileyard Education and TY-e will ensure all personal data:

- Will be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Section 9.0 is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 9.1 is also met (see Conditions for Processing, below)
- Will be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes
- Will be relevant and not excessive with respect to the purposes for which it is processed
- Will be accurate and, where appropriate, kept up-to-date;
- Will be kept for no longer than is necessary in light of the purpose(s) for which it is processed
- Will be processed in accordance with the rights of data subjects under the Act

- Shall be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and
- Shall not be transferred to a country or territory outside of the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

PROCEDURE

Tileyard Education's designated **Data Controller** is the Tileyard Education Manager. They exercise the following responsibilities on behalf of the Managing Director:

- Ensuring that staff, students and authorised third parties comply with the data protection principles, and GDPR requirements as set out in legislation, in respect of personal data under their control
- Ensuring that the Tileyard Education's Data Protection Manual is appropriate for the types of personal data being processed

- Ensuring that Tileyard Education maintains an up-to-date notification of its use of personal data with the Information Commissioner's Office .

Tileyard Education's designated **Data Protection Officer** is the Tileyard Education Manager. They are responsible for:

- Training and advising staff on the implementation of Tileyard Education Data Protection Manual and GDPR requirements
- Monitoring compliance with the Tileyard Education's Data Protection, Employee Records Data Protection, Data Security and Freedom of Information policies.
- Serving as the focal point for the administration of all subject access requests relating to personal data held by Tileyard Education

A Data Owner is defined by the Act as a member of staff given authorised access to data which relates to a living individual who can be identified from that data or from that data as well as other information which is in the possession of, or is likely to come into the possession of, the data controller (including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual).

Data Owners are responsible for:

- Ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes
- Ensuring that the security measures are appropriate for the types of personal data being processed

Data Subjects, whether staff, students or authorised third parties are responsible for:

- Ensuring that any personal information that they provide to Tileyard Education in connection with their employment, registration or other contractual agreement is accurate to the best of their knowledge
- Informing Tileyard Education of any changes to any personal information which they have provided, e.g. changes of address
- Responding to requests to check the accuracy of the personal information held on them and processed by Tileyard Education details of which will be sent out from time to time, and informing Tileyard Education of any errors that need amending

- As a Data Controller, Tileyard Education is required to notify the Information Commissioner's Office that it is processing personal data.

- Data Controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify is a criminal offence.
- Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.
- The Managing Director, via the Tileyard Education Manager, shall be responsible for notifying and updating the Information Commissioner's Office.

Data Types

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines "**sensitive personal data**" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Tileyard Education only holds personal data which is directly relevant to its dealings with a given data subject.

The following data may be collected, held and processed by Tileyard Education from time to time.

- **Staff, Agent and Contractor Administration**; Personal Details, Salary, contractor's fees and remuneration details, Family, Lifestyle & Social Circumstances, Education & Training Details, Employment Details, Financial Details, Goods or Services Provided, Racial or Ethnic Origin, Trade Union Membership, sexual orientation, Physical or Mental Health Conditions and disabilities and how they may affect individuals, Offences (Including Alleged Offences)
- **Advertising, Marketing, Public Relations**; General Advice Services, Personal Details, Family, Lifestyle & Social circumstances, Education & Training Details, Employment Details, Physical or Mental Health Conditions, Text of Magazine Articles Processing Personal Data, photographs
- **Accounts & Records**; Personal Details, Employment Details, Financial Details, Goods or Services Provided

- **Education and Personal details**; Family, Lifestyle & Social Circumstances, previous education & training Details, Employment Details
- **Financial Details;** Racial or Ethnic Origin, Religious or Other Beliefs of a Similar Nature, Physical or Mental Health Condition, Offences (Including Alleged Offences), Student Records
- **Student & Staff Support Services**; Personal details, Family, Lifestyle & Social Circumstances, Education & Training Details, Employment Details, Financial Details, Goods or Services Provided, Racial or Ethnic Origin, Religious or Other Beliefs of a Similar Nature, Trade Union Membership, Physical or Mental Health Conditions or disabilities and how they may affect individuals
- **Crime Prevention and Prosecution of Offenders**; Personal Details, Goods of Services Provided, Offences (Including Alleged Offences)
- **Criminal Proceedings, Outcomes & Sentences**, Visual Image, Personal Appearance & Behaviour

All personal data held by Tileyard Education is collected in order to ensure that Tileyard Education can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. Personal data shall also be used by Tileyard Education in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within Tileyard Education. Personal data may be passed from one department to another in accordance with the data protection principles. Under no circumstances will personal data be passed to any department or any individual within Tileyard Education that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed**.**

Processing Personal Data
Tileyard Education shall ensure that:

- All personal data collected and processed for and on behalf of Tileyard Education by any party is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- Data subjects are informed of their responsibility to ensure that their personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed

- Personal data is held for no longer than necessary in light of the stated purpose(s)
- Sensitive Personal data is held in a safe and secure manner (and not on the Shared Drive), taking all appropriate technical and organisational measures to protect the data
- Personal data is transferred using secure means, electronically or otherwise
- Personal data is not transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- Data subjects can exercise their rights (as set out more fully in the act), to request any information or kept by Tileyard Education

Conditions for Processing
At least one of the following conditions must be met whenever Tileyard Education processes personal data:

- The individual to whom the personal data refers has consented to the processing
- The processing is necessary in relation to a contract which the individual has entered into or because the individual has asked for something to be done so they can enter into a contract
- The processing is necessary because of a statutory obligation that applies to an individual
- The processing is necessary to protect the individual's "vital interests"; this condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition

In addition to the conditions described, at least one of the following conditions must also be met whenever Tileyard Education processes sensitive personal data:

- The individual who the sensitive personal data refers to has given explicit consent to the processing
- The processing is necessary to comply with employment law
- The processing is necessary to protect the vital interests of the individual (in a case where the individual's consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld)
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents
- The individual has deliberately made the information public
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights
- The processing is necessary for administering justice, or for exercising statutory or governmental functions
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals

Organisational Measures

Tileyard Education shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A Data Protection Officer will be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education will be furnished with a copy of this Data Protection Manual
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education will be made fully aware of both their individual responsibilities and Tileyard Education responsibilities under the Act
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education handling personal data will be appropriately trained to do so
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education handling personal data will be appropriately supervised
- Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed
- The performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education handling personal data will be regularly evaluated and reviewed
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education handling personal data will be bound to do so in accordance with the principles of the Act and this Data Protection Manual by contract; failure by any employee to comply with the principles or this Data Protection Manual shall constitute a disciplinary offence; failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Data Protection Manual shall constitute a breach of contract; in all cases, failure to comply with the principles or this Data Protection Manual may also constitute a criminal offence under the Act

- All contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Tileyard Education arising out of this Data Protection Manual and the Act
- Where any contractor, agent, consultant, partner or other party working on behalf of Tileyard Education handling personal data fails in their obligations under this Data Protection Manual that party shall indemnify and hold

harmless Tileyard Education against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

Rights of Data Subjects

Under the Act, Data Subjects have:

- The right to be informed that their personal data is being processed
- The right to access any of their personal data held by Tileyard Education within 40 calendar days of making a request
- The right to prevent the processing of their personal data in limited circumstances
- The right to rectify, block, erase or destroy incorrect personal data

Access by Data Subjects

A Data Subject may make a subject access request ("SAR") at any time to see the information which Tileyard Education holds about them

SARs must be made in writing, accompanied by the correct fee; Tileyard Education currently requires a fee of £10.00 (the statutory maximum) for all SARs excluding credit file requests (which attract a fee of £2.00).

Upon receipt of a SAR Tileyard Education shall have a maximum period of 40 working days within which to respond. The following information will be provided to the data subject:

- Whether or not Tileyard Education holds any personal data on the data subject
- A description of any personal data held on the data subject
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to
- Details of any technical terminology or codes

EMPLOYEE RECORDS DATA PROTECTION POLICY

Tileyard Education collects employee related personal data in order to ensure that Tileyard Education can effectively manage and facilitate efficient transactions with its employees and contractors as well as to comply with relevant employment law. Tileyard Education has no Human Resources Manager so the responsibility for this lies with the Managing Director. He will be the primary handler and administrator of all subject access requests relating to personnel data held by Tileyard Education.

The Employee Records Data Protection Policy does not form part of the formal contract of employment and/or service provision, but it is a condition of engagement that all employees/contractors will abide by it at all times.

PROCEDURE

Monitoring

Tileyard Education may from time to time monitor the activities of employees; such monitoring may include, but will not necessarily be limited to, internet and email monitoring.

Any employee that is to be monitored shall be informed in advance of such monitoring; however, under no circumstances will monitoring interfere with an employee's normal duties.

Tileyard Education shall use its best and reasonable endeavors to ensure that there is no intrusion upon employees' personal communications or activities and **under no circumstances will monitoring take place outside of the employee's normal place of work or work hours.**

Benefits

In cases where employees are enrolled in benefit schemes that are provided by Tileyard Education (including, but not limited to, pensions and healthcare) it may be necessary from time to time for third party organisations to collect personal data from relevant employees.
Prior to collection, employees will be fully informed of the personal data that is to be collected, the reasons for its collection, and the ways) in which it will be processed.

Tileyard Education shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

Health Records

Tileyard Education holds health records on all employees in order to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records include details of sick leave, medical conditions, disabilities and prescribed medication are kept by the Managing Director.
Data under this heading will be used by management only and will not be revealed to fellow employees and peers (unless those employees are responsible for health records in the normal course of their duties).

Employees and contractors have the right to request that Tileyard Education does not keep health records on them. All such requests must be made in writing and addressed to the Managing Director

Employee Records and Retention

Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes (normally six years following the cessation of the working relationship) or as required to comply with legislation.

DATA SECURITY POLICY

Tileyard Education collectively, and its staff and students individually, are responsible for ensuring that appropriate technical and organisational measures are taken against the unauthorised or unlawful processing of personal data as well as against accidental loss or destruction of, or damage to, personal data.

PROCEDURE

Tileyard Education staff and students must ensure that they employ safeguards for personal data that is proportional to the risks presented in their processing activities.

Any staff or students who discover a potential or actual security breach must immediately inform the Managing Director.

Tileyard Education will ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of Tileyard Education comply with the following when processing and / or transmitting personal data:

- All emails containing personal data will be encrypted
- Personal data may only be transmitted over secure networks; transmission over unsecured networks is not permitted under any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely; the email itself, and any temporary files associated therewith, should be deleted
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; the use of an intermediary is not permitted
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; the use of portable storage devices is not permitted.
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised

FREEDOM OF INFORMATION POLICY

The Freedom of Information Act 2000 imposes upon all public sector institutions an obligation to provide the public with wide rights of access to their records and guarantees the public a statutory right to:

- Obtain (either from Tileyard Education's website or in some other form) all the information covered by the organisation's Publication Scheme
- Request (within the limitations outlined in the Data Protection Act 1998) any information held by the organisation, regardless of when it was created, by whom, or the form in which it is now recorded

As a private sector institution with quasi-public sector functions, Tileyard Education is not bound by the Freedom of Information Act 2000; however, Tileyard Education is committed to being open and honest in the conduct of its operations. To this end, Tileyard Education will:

- Be open with the general public and the media and will place in the public domain as much information about its activities as is practicable

Tileyard Education and TY-e

E-Safety Policy & Procedures

Last update: May 2017

Review Date: April 2019

Contents

1. CYP E-Safety Policy ..... **Error! Bookmark not defined.**

2. E-Safety leads ..... **Error! Bookmark not defined.**

3. Risks and Issues ..... **Error! Bookmark not defined.**

3.1. WHAT TO DO IF A CHILD'S AT RISK Flowchart ..... **Error! Bookmark not defined.**

4. Vulnerability of Some Groups of Children ..... **Error! Bookmark not defined.**

5. Cyberbullying ..... **Error! Bookmark not defined.**

6. Acceptable Use Policy (AUP) ..... **Error! Bookmark not defined.**

7. Forms .....

FORM A – STAFF / VOLUNTEERS ACCEPTABLE USE POLICY .... **Error! Bookmark not defined.**

FORM B – CHILDREN AND YOUNG PEOPLE'S ACCEPTABLE USE AGREEMENTS ..... **Error! Bookmark not defined.**

FORM C: E-SAFETY INCIDENT MONITORING FORM ..... **Error! Bookmark not defined.**

FORM D: E-SAFETY TRAINING RECORDS ..... **Error! Bookmark not defined.**

FORM E: E-SAFETY ORGANISATION CHECKLIST ..... **Error! Bookmark not defined.**

APPENDIX 1 - E-SAFETY TIPS FOR ADULTS WORKING WITH CHILDREN AND YOUNG PEOPLE ..... **Error! Bookmark not defined.**

APPENDIX 2 - PARENTS' / CARERS' INFORMATION ..... **Error! Bookmark not defined.**

APPENDIX 3 - USEFUL CONTACTS/WEBSITES ..... **Error! Bookmark not defined.**

APPENDIX 4 - GLOSSARY OF TERMS ..... **Error! Bookmark not defined.**

1. TILEYARD EDUCATION AND TY-E E-Safety Policy

TILEYARD EDUCATION AND TY-E's E-Safety policy and procedures apply to all staff, contractors, tutors, volunteers, trustees, children, young people and anyone working on behalf of TILEYARD EDUCATION AND TY-E.

The aim of the policy is to:

- **Protect children and young people who receive TILEYARD EDUCATION AND TY-E's services and who make use of information and communication technology (such as mobile phones, games consoles and the internet) as part of their involvement with TILEYARD EDUCATION AND TY-E.**
- **Provide staff and volunteers with the principles that guide TILEYARD EDUCATION AND TY-E's approach to E-Safety.**
- **Protect professionals.**
- **Ensure that, as an organisation, TILEYARD EDUCATION AND TY-E operate in line with our values and within the law in terms of how we use information technology.**

This E-Safety Policy is to be read in conjunction with TILEYARD EDUCATION AND TY-E's Safeguarding and Child Protection Policy.

TILEYARD EDUCATION AND TY-E recognises that the welfare of the children/young people who come into contact with our services is paramount and governs our approach to the use and management of information and communication technologies ("ICT").

TILEYARD EDUCATION AND TY-E will promote E-Safety by:

- **Appointing an E-Safety Coordinator – Harry Leckstein**

- **Having procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT.**

- **Supporting and encouraging the children and young people using our service to use the opportunities offered by mobile phone technology and the internet in a way that keeps them safe and shows respect for others.**

- **Educating and providing information for parents on e-safety.**

- **Supporting and encouraging parents and carers to keep their children safe online and when using their computers, mobile phones and game consoles.**

- **Incorporating statements about safe and appropriate ICT use into the codes of conduct for staff and volunteers and for children and young people.**

- **Having an e-safety agreement with children and young people.**
- **Using our procedures to deal with any inappropriate ICT use, complaints and/or allegations by anyone working for TILEYARD EDUCATION AND TY-E or using TILEYARD EDUCATION AND TY-E's services.**

- **Informing parents and carers of incidents of concern as appropriate.**

- **Regularly reviewing and updating the security of our information systems.**

- **In the event of a suspected breach of E-Safety, the E-Safety coordinator to investigate.**

- **Ensuring that images of children, young people and families are only used after their written permission has been obtained from their parents or guardians, and only for the purpose for which consent has been given.**

TILEYARD EDUCATION AND TY-E will handle complaints regarding E-Safety by:

Taking all reasonable precautions to ensure E-Safety.

Giving staff/volunteers, contractors and children/young people information about infringements in use and possible sanctions.

Sanctions include:

- **Interview with a member of staff or contractor**
- **Informing parents/carers**
- **Removal of mobile phone, internet or computer access for an agreed period of time**
- **Referral to local authority/police**

The E-Safety coordinator Harry Leckstein will be the first point of contact for any complaint. Any complaint about staff/volunteer's misuse will be referred to the relevant E-Safety lead and may result in formal disciplinary proceedings. Any complaint about the E-Safety coordinator will be referred to the Company Secretary and may result in formal disciplinary proceedings.

If the relevant E-Safety Coordinator is not available, the complaint to be referred to the Chair of Trustees. Complaints of cyber-bullying are dealt with in accordance

with TILEYARD EDUCATION AND TY-E's Behaviour and Safeguarding and Child Protection Policies.

Concerns related to child protection are dealt with in accordance with the London Safeguarding Children Board's child protection procedures at www.islingtonscb.org.uk

2. E-Safety Officers contact details

All TILEYARD EDUCATION AND TY-E Sessions – Harry Leckstein, harry@tileyard.co.uk / tel +44 (0)7796 950 406

The responsibilities of these roles are to:

- **Develop an E-Safety culture.**
- **Be the named points of contact on all E-Safety issues.**
- **Monitor E-Safety.**
- **Ensure that everyone: staff/volunteers, children/young people, management committee members and Trustees know what to do if they are concerned about an E-Safety issue.**
- **Keep abreast of developing E-Safety issues via**

http://www.islingtonscb.org.uk/key-practice-guidance/Pages/E-Safety.aspx

- **Ensure that E-Safety is embedded within continuing professional development (CPD)for staff/volunteers.**
- **Co-ordinate training as appropriate.**
- **Ensure that E-Safety is embedded across all activities as appropriate.**
- **Ensure that E-Safety is promoted to parents/carers, other users and children/young people.**
- **Ensuring that the infrastructure and technology provide a safe and secure environment for children/young people.**
- **Maintain an E-Safety incident log to record incidents and concerns.**
- **Monitor and report on E-Safety issues to the management team and management committee.**
- **Review and update E-Safety policies and procedures on a regular basis and after an incident.**

3. Risks and Issues

The following are the range of technologies children/young people and staff/volunteers use positively but which can also put them at risk:

- **Internet**
- **E-mail**
- **Instant messaging Blogs**
- **Podcasts**
- **Social networking sites**
- **Chat rooms**
- **Gaming Sites**
- **Mobile phones with camera and video functionality**
- **Mobile technology (eg games consoles) that are internet ready and include webcams**
- **E-smart phones with e-mail, web functionality, camera and video functionality and secure text network**

Risks can come under the categories outlined below:

	Commercial	Aggressive	Sexual	Values
Content That the user may come across either accidentally or via a deliberate search	**Adverts Spam Sponsorship Requests for personal information Exposure to age-inappropriate material**	**Violent/hateful content**	**Exposure to illegal material, eg, images of child abuse Pornographic/ unwelcome sexual content**	**Bias Racist Misleading informatio n/ advice**
Contact Unsuitable contact from another user	**Tracking Harvesting Publishing information about themselves**	**Being bullied, harassed, stalked**	**Meeting strangers Being groomed**	**Self-harm Unwelcom e persuasion s**
Conduct	**Illegal downloading Gambling**	**Bullying or harassing another**	**Creating and uploading inappropriate/**	**Providing misleading**

User's behaviour that creates risk either through illegal activity or lack of awareness of the potential consequences	**Hacking Financial scams**		**abusive material 'Sexting'**	**information/ advice**

4. Vulnerability of Some Groups of Children

Some groups of children are more vulnerable to being abused through the use of technology and are less resilient to deal with it. Technology can also increase their offline vulnerability. These children need further protection to keep them safe.

These groups of children include:

- **Looked After Children. There is evidence that children who are looked after and children who are adopted are using social networking sites to access their birth families, and birth families are using social networking sites to contact their children, even though there may be a court order prohibiting any contact. This results in unmediated contact.**
- **Children with disabilities. Studies have shown that pupils with Special Educational Needs are 16% more likely to be persistently cyber bullied over a prolonged period of time. These children may be more socially naïve.**
- **Children living away from their families can make them more vulnerable, for example, children living in residential units, boarding school, privately fostered.**
- **Children at risk of sexual exploitation. Technology is used to contact, groom and control these children. Research states that it has been rare to identify cases of child sexual exploitation where the use of technology has not been a factor. For more information about children at risk of sexual exploitation refer to ISCB's website: http://www.islingtonscb.org.uk/key-practice-guidance/Pages/Sexual-Exploitation.aspx .**
- **There is general risk to adolescent girls with the proliferation of websites aimed at them that promote anorexia, related eating disorders and 'starving for perfection'.**
- **There is general risk to boys who can be at high risk of addiction to violent games and pornography.**

5. Cyberbullying

What is cyberbullying?

Cyberbullying is the use of technology such as mobile phone, internet, e-mail, social networking sites, chat rooms and instant messaging services to deliberately upset someone else.

- **It can be used to carry out all the different types of bullying, an extension of face-to-face bullying.**
- **It can also go further, by invading home/personal space and can involve a greater number of people.**
- **It is an anonymous method by which bullies can torment their victims at any time of day or night.**
- **It can draw bystanders into being accessories.**
- **It includes: threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images ('happy-slapping'); and manipulation.**
- **It includes sexting, sending explicit images electronically. These images can be widely distributed**
- **It also includes trolling, the online posting of inflammatory messages with the intention of provoking an emotional response. This can involve violent threats, poking fun, making trouble and causing annoyance.**
- **It can involve setting up hate websites or groups on social networking sites.**
- **It can take place across age groups and adults working with children can be targeted, for example, by pupils and/or parents.**

Impact on the victim

The victim may receive email, chat, text messages or posts on social networking sites that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Cyberbullying can pose a serious threat to their physical and emotional safety.

Responding to cyberbullying

TILEYARD EDUCATION AND TY-E will address all incidents of bullying thoroughly and sensitively.Victims of cyber bullying will be offered the immediate opportunity to discuss the matter with a member of staff who will reassure the child and offer support.
They will be reassured that what they say will be taken seriously and handled sympathetically.

Staff will support the individual who has been cyber bullied. Keeping them under close supervision and checking their welfare regularly.
Children who have been perpetrators of cyber-bullying will be helped by discussing what has happened, establishing why the child became involved. Staff will help the child to understand why this form of behavior is unacceptable and will encourage him/her to change their behavior.

If the cyber-bullying behavior persists, more serious actions may have to be taken which may involve consultation with parents and suspension or exclusion.

In all cases of cyberbullying TILEYARD EDUCATION AND TY-E will ensure that the evidence is preserved.

TILEYARD EDUCATION AND TY-E will respond as follows to cases of cyberbullying:

- **Change or if not possible encourage the victim to change their mobile phone number.**
- **Report the bullying to the site where it was posted.**
- **Try to get content removed from the web.**
- **Investigate the possibility of the victim blocking the person bullying from their sites and services.**
- **Ask the person bullying to delete the offending content and say who they have sent it on to.**
- **Contact the police in cases of actual/suspected illegal content.**
- **Consider the bystanders who can amount to hundreds of young people.**

6. Acceptable Use Policy (AUP)

TILEYARD EDUCATION AND TY-E's AUP clearly identifies the expectations and boundaries for the use of technology both provided by TILEYARD EDUCATION AND TY-E and those provided by individuals for their personal use.

AUP applies to the use of computers, laptops, mobile phones, smart phones, cameras and video cameras, webcams, games consoles and other technology that may be available within the organisation.

TILEYARD EDUCATION AND TY-E Staff/volunteers and users should be aware of the potential consequences of any breach of the AUP.

TILEYARD EDUCATION AND TY-E will deliver/access e-safety awareness raising and training for staff/volunteers and users.

For the workforce - staff/volunteers:

- **Induction of new staff/volunteers will include information on E-Safety and the associated policies.**
- **TILEYARD EDUCATION AND TY-E staff/volunteers will receive training that includes how to differentiate between their personal and professional behaviour especially when they are online.**
- **TILEYARD EDUCATION AND TY-E will develop appropriate strategies for the safe and responsible use of technology as part of the workforce's everyday practice.**
- **All staff/volunteers must sign an AUP contract.**
- **Monitor your workforce's internet use if possible.**
- **Report any issues that arise as a result of monitoring to STILEYARD EDUCATION AND TY-E's named E-Safety persons.**

For children/young people:

- **Include children/young people in developing E-Safety policies where possible.**
- **Children/young people that use TILEYARD EDUCATION AND TY-E's ICT must sign an AUP contract.**

Parents and carers

Raise parents/carers' awareness of E-Safety through training, where appropriate, and displaying/distributing information.

7. FORM A – STAFF / VOLUNTEERS ACCEPTABLE USE POLICY

This agreement covers the use of digital technologies in TILEYARD EDUCATION AND TY-E including email, internet, intranet, network resources, software, equipment and systems.

I will only use TILEYARD EDUCATION AND TY-E's digital technology resources and systems for professional purposes.

I will not reveal my password(s) to anyone.

I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.

I will not use anyone else's password if they reveal it to me and will advise them to change it.

I will not allow unauthorised individuals to access any TILEYARD EDUCATION AND TY-E systems.

I will ensure all documents, data, etc are saved, accessed and deleted in accordance with TILEYARD EDUCATION AND TY-E's network and data security and confidentiality protocols.

I will not engage in any online activity that compromises my professional responsibilities.

My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods.

I will only use the approved email system for any email communication related to work at TILEYARD EDUCATION AND TY-E.

I will not browse, download or send material that could be considered offensive to colleagues and users.

I will report any accidental access to or receipt of inappropriate materials, or filtering breach to the responsible E-Safety coordinator Harry Leckstein.

I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.

I will not publish or distribute work that is protected by copyright.
I will not connect a computer, laptop or other device (including USB flash drive) to the computers/internet that does not have up-to-date anti-virus software.

I will not use personal digital cameras or camera phones for taking and transferring images of children/young people or staff/volunteers without written permission and will not store images at home.

I will ensure that any private social networking sites/blogs, etc that I create or actively contribute to are separate from my professional role.
It is my responsibility to ensure that my use of social networking sites/blogs, etc does not compromise my professional role, eg, setting appropriate security settings.

Any computer or laptop loaned to me by TILEYARD EDUCATION AND TY-E is provided solely for professional use

I will access TILEYARD EDUCATION AND TY-E's resources remotely (such as from home) only through approved methods and follow E-Security protocols to access and interact with those materials.

Any confidential data that I transport from one location to another will be protected by encryption.

I will follow TILEYARD EDUCATION AND TY-E's data security protocols when using confidential data at any location.

Any information seen by me with regard to service users held within TILEYARD EDUCATION AND TY-E will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

It is my duty to support a whole organisation safeguarding approach and I will alert the named Safeguarding/Child Protection officer or Chair if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern.

I will not use, access or set up a Facebook or any other social networking site to follow a child's/parent's/carer's movements or activities. I will not monitor or investigate their social networking sites. If I come across a child's/parent's/carer's social networking account or site I will not enter it. If I have Safeguarding/Child

Protection concerns about a child's/young person's behaviour on-line, or if I think social media could provide critical information, for example, if a child is missing or is at risk of harm, I will contact the police and children's social care.

It is my responsibility to ensure that I remain up-to-date, read and understand TILEYARD EDUCATION AND TY-E's most recent E-Safety policies.

I understand that all internet/network usage can be logged and this information can be made available to my manager on request.
I understand that failure to comply with this agreement could lead to disciplinary action

I agree to abide by this agreement.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Authorised Signature

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

FORM B – CHILDREN AND YOUNG PEOPLE'S ACCEPTABLE USE AGREEMENTS

B.1 FOR PEOPLE OF 13 OR OVER

This agreement covers the use of digital technologies in TILEYARD EDUCATION AND TY-E including email, internet and equipment ("ICT").

- **I will use TILEYARD EDUCATION AND TY-E's ICT systems in a responsible way, to ensure that there is no risk to my safety, the safety of others or to the safety and security of the ICT systems.**

- **TILEYARD EDUCATION AND TY-E may monitor my use of the ICT systems, email and other digital communications.**

- **I will not share my password nor will I try to use any other person's username and password.**

- **I will not disclose or share personal information about myself or others when on-line.**

- **If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.**

- **I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I will report this to the Youth Worker in Charge or if unavailable to the E-Safety Co-ordinator Stephen Griffith or Trustee responsible for E-Safety**

- **I will not use TILEYARD EDUCATION AND TY-E's ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).**

- **I will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.**

- **I will not use strong, aggressive or inappropriate language when I communicate with others.**

- **I will not take or distribute images of anyone without their permission.**

• If I use my own devices (Mobile phone) in TILEYARD EDUCATION AND TY-E I will follow the rules set out in this agreement, in the same way as if I was using TILEYARD EDUCATION AND TY-E's equipment.

• I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others.

• I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to these materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email because of the risk of the attachment containing viruses or other harmful programmes.

• I will not install or attempt to install programmes of any type on any equipment or store programmes in a computer.

• I will not try to alter computer settings.

• I will only use chat and social networking sites with permission and at the times that are allowed.

• Where work is protected by copyright, I will not try to download copies, including music and videos.

I have read and understand the above and agree to follow these guidelines.

FULL NAME……(printed)

Signature ..... Date .....

FORM C: E-SAFETY INCIDENT MONITORING FORM

Details of person completing the form **Name:** **Phone number:** **Email:**
Date of incident:
Where did the incident take place?
Names of those involved in the incident:
Age(s) of child(ren) involved:
Was the incident? **Child on Child☐ Child on Adult☐ Adult on Child☐ Adult on Adult☐**
Type of incident **Sexual☐ Grooming☐ Bullying☐ Violence☐ Hate/incitement☐ Financial☐** **Other☐** **Please give details:**
What media was used? **Social networking☐ BBM or other free system☐ MSN☐ Email☐ Webcam☐** **Mobile Phone☐ Games Console☐** **Other☐ Please specify:**
What action was taken in relation to those involved in the incident? **Please give details:**
What follow-up action was taken? **Referral to LADO☐ Referral to Children's Social Care☐ Advice to parents☐** **Police investigation☐** **Other☐** **Please give details:**

FORM D: E-SAFETY TRAINING RECORDS

NAME	COURSE	DATE	MANAGER'S SIGNATURE

APPENDIX 1 - E-SAFETY TIPS FOR ADULTS WORKING WITH CHILDREN AND YOUNG PEOPLE

Set your privacy setting to "Just Friends" so that your details, photographs, location, etc can only be seen by your invited friends.

Have a neutral picture of yourself as your profile image.

Don't post potentially embarrassing material.

Reject or ignore friendship requests unless you know the person or want to accept them.

Choose your social networking friends carefully and ask about their privacy controls.

Do not accept 'friendship requests' on social networking or messaging sites from children/young people (or their parents) that you work with.

For groups and networks set your privacy setting to private or everyone in the group or network will be able to see your profile.

If you wish to set up a social networking site for a work project create a new user profile for this. Do not use your own profile.

Use location settings wisely. Many social networking and online applications disclose your location. Where this is specifically linked to your identity it will, within a couple of days have disclosed where you live and when you are not at home.

There are social networking groups to bring together people sharing experiences, such as attending festivals and conferences. This advertises when you will not be at home.

Be careful not to leave your Facebook account logged-in in a shared area/household. Someone could leave status messages that may compromise or embarrass you. This is called Frape (Facebook Rape) and can be a form of cyber-bullying.

If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name

Think before you post. Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a "web crawler" and it will always be there.

Be aware of addictive behaviour. Adults are just as likely as young people to get hooked on social networking, searching or games.

When you log-into a web site, unless your computer is exclusive to you, do not tick boxes that say 'remember me'.

Do not leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.

Use strong passwords that include a mixture of upper and lower case letters, numbers and other characters, are a minimum of 8 characters in length and do not contain the person's username. Do not to use the 'Remember Password' feature of applications.

Turn Bluetooth off when you are not using it. If you open un-pass worded Bluetooth anyone with Bluetooth in range can read the content of your phone or device.

Lock your mobile. Set a pin number or password for your mobile phone. With access to email, social networking and contacts an unlocked mobile phone can put your identity, and others, at risk.

APPENDIX 2 - PARENTS' / CARERS' INFORMATION

E-safety is concerned with safeguarding children in the early years age range in the digital world. It is about learning to understand and use new technologies and Information Communication Technology in a positive way. E-Safety is not about restricting children, but educating them about the risks as well as the benefits so they can feel confident and happy online.

To keep your children safer online:

- **Know what your child is doing online much like you would offline.**
- **Make an effort to get computer literate if you want to support and understand your children, you need to have a reasonable understanding of their world.**
- **Talk to your child. Share the experience with them and ask them to show you how they use technology.**
- **Be open and encourage them to talk to you.**
- **Establish how the internet will be used in your house.**
- **Agree the type of content that you would be happy for them to download, knowingly receive or send on to others.**
- **Discuss what will be kept private online, eg, information, bank and credit card details and photos.**
- **Encourage balanced use – switching off at mealtimes, bedtime.**
- **Use a child friendly search engine.**
- **Install antivirus software, filtering and firewalls.**
- **Secure your internet connections.**
- **Use parental control functions for computers, mobile phones and games consoles.**
- **Remember that tools are not always 100% effective and sometimes things can get past them. Locate the computer/laptop in a family room and don't allow webcams to be used unless with your consent and always in a family room under supervision.**
- **Encourage your child not to hesitate about coming to you about anything they see online which upsets or disturbs them.**
- **If your child reports a problem make sure you support them, report it or seek advice.**
- **Save any abusive messages or inappropriate images for evidence purposes.**
- **Be aware of how to report nuisance calls or texts.**

APPENDIX 3 - USEFUL CONTACTS/WEBSITES

Katy Potts – for advice on E-safety training and policy implementation.	**katy.potts@islington.gov.uk**

Websites

BBC Learning zone	**www.bbc.co.uk/learningzone/clips/5594.flv**
Child Exploitation and Online Protection Centre (CEOP)	**http://ceop.police.uk/**
Childnet International	**http://www.childnet-int.org**
Cyberbullying	**www.digizen.org**
Cybermentors	**https://cybermentors.org.uk/**
Get Safe Online	**http://www.getsafeonline.org/**
Information Commissioner's Officer	**http://ico.org.uk/for_organisations/data_protection/**
Islington Safeguarding Children Board – E-safety page	**http://www.islingtonscb.org.uk/key-practice-guidance/Pages/E-safety.aspx**
Internet Watch Foundation To report indecent content.	**http://www.iwf.org.uk/**
***Kidsmart**	**http://www.kidsmart.org.uk/**
***KnowItAll (KIA)**	**www.childnet-int/kia)**
Ofsted	**http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies**
Safe network	**http://www.safenetwork.org.uk/Pages/default.aspx**
***ThinkuKnow (TUK)**	**www.thinkuknow.co.uk**
UK Council for Child Internet Safety (UKCCIS)	**http://www.education.gov.uk/ukccis/**
UK Safer Internet Centre 10am-4pm helpline. The professional online safety helpline can escalate a report with Facebook and other social networking sites where content needs to be removed urgently	**http://www.saferinternet.org.uk http://www.saferinternet.org.uk/helpline Tel 08443814772**
Vodafone have published useful guides to parents on E-Safety. The latest (April 14) available from link here:	**http://www.vodafone.com/content/parents/digital-parenting/view_magazines.html**
Wise Kids – promoting innovative positive and safe internet use.	**www.wisekids.org.uk**
Online Compass Tool	**www.onlinecompass.org.uk**
Online Safety; A Toolkit for Early Years Settings	**www.plymouth.gov.uk/early_years_toolkit.pdf**

***These websites contain activities to teach children about E-safety**

APPENDIX 4 - GLOSSARY OF TERMS

Age related filtering	**Differentiated access to online content dependent on age and appropriate need**
AUP	**Acceptable Use(r) Policy**
Blogging & social networking	**Anyone can produce and distribute their own content and link with other sites to create a very powerful network for sharing ideas and influence opinion**
CEOP	**Child Exploitation and Online Protection centre**
Cyber bullying	**Bullying using technology such as computers and mobile phones**
Downloading	**Receiving information or data electronically usually through the internet; this could include saving a document, picture, music or video from a website**
Encryption	**Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device**
E-safety	**Limiting risks to children/young people when using Information and Communications Technology (ICT). E-safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT: fixed or mobile, current, emerging and future ICT**
Filtering	**Software that can help to block a lot of inappropriate material but they are not 100% effective**
Firewall	**A buffer between your computer and the internet. It limits incoming and outgoing information, and keeps your computer safe from intruders. It can't stop you downloading spyware, but it can alert you if a program is sending information over the internet without your permission**
Frape	**Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset**
Games Console	**Examples include XBOX 360, Nintendo Wii, PlayStation 3, Nintendo DS**
Grooming	**Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'**
Hacking	**When your details, online accounts or other personal information is accessed by a stranger**

ICT	**Information and Communications Technology, eg, mobile phones, gaming consoles, computers, email, social networking**
Identity Theft	**When your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud or deception**
ISP	**Internet Service Provider. A company that connects computers to the internet for a fee**
Lifestyle website	**An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide**
Locked down system	**In a locked down system almost every website has to be unbarred before it can be used. Only vetted websites can be accessed**
Malware	**Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses)**
Managed system	**In a managed system the organisation has some control over access to websites and ideally offers age-appropriate filtering**
Password - strong	**A strong password contains a mixture of upper and lower case letters, Numbers and other characters. It is recommended to be a minimum of 8 characters in length**
Phishing	**Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen**
Profile	**Personal information held by the user on a social networking site**
RUP	**Responsible Use(r) Policy**
Safer Internet Day	**Initiated by the European Commission and on the second day, of the second week of the second month each year.**
Sexting	**Sending and receiving of personal, sexual images or conversations to another party, usually via mobile phone or instant messaging**
SHARP	**Example of an anonymous online reporting mechanism (Self Help And Reporting Process)**
SNS	**Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people**

Spam	**An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email)**
Spyware & adware	**A general term for malicious software that is designed to take control of a computer without the consent of the user. Adware is one type of spyware - computer programs in which commercial advertisements are automatically shown to the user without their consent**
Trojan	**A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers**
Trolling	**Posting inflammatory messages with the intention of provoking an emotional response**
Uploading	**Sending and saving information or data from a local system, eg, mobile phone or computer, to a remote system, eg, a website**
URL	**Universal Resource Locator or website address**
VOIP	**Voice Over Internet Protocol**
Youtube	**Social networking site where users can upload, publish and share videos**