Tileyard Education
Diversity, Inclusion and Equality Mission Statement

Tileyard Education is committed to providing and upholding academic and educational excellence that fosters best practice and learning, centred around equal access to industry-leading tuition, facilities, professional networks, mentoring and career pathway progression.

Tileyard Education
Equality, Diversity and Inclusivity Manifesto Pledges 2023

Tileyard Education commit to the following manifesto for Equality, Diversity and Inclusivity:

We are committed to cultivating a transparent, safe and consciously inclusive culture for all staff, faculty, students and alumni. We will provide and uphold academic and educational excellence that fosters best practice and learning, centred around equal access to industry-leading tuition, facilities, professional networks, mentoring and career pathway progression.

We will build diverse new partnerships from within the Tileyard Community and continue to develop coalition partnerships with national and international institutions that broaden and increase participation and accessibility of educational opportunities to a diverse audience. To date these include MTNNOw, Yorkshire Sound Women's Network, Small Green Shoots, The Avenue Youth Project and SoundSkool.

We will upskill our faculty through externally delivered continued professional development that is specifically designed to foster an increasingly transparent and consciously inclusive workplace, and to celebrate the diversity of our student body by prioritising platforms for celebrating diversity.

We will annually review our internal policies and procedures to ensure that equality, diversity and inclusion are embedded into every policy decision we make. TYE acknowledge that marginalised groups experience barriers to entry and commit to investigating the nature of these barriers and legislating to mitigate them in a sustained and meaningful way.

We will continue to identify barriers to entry and inclusion within HIgher Education and the creative industry workplace and will lobby and action for wider awareness and inclusion wherever possible, including through our membership of the UK Music Academic Partnership and our embedded relationships with validating partners Nottingham Trent University and University of Wales Trinity Saint David.

Our senior leadership commit to raising awareness of EDI reviews and outcomes through internal communications and via external marketing channels to increase transparency and highlight the actions we are taking to forefront the importance of equality, diversity and inclusion to the institution.

TYE renew our commitment to ensuring all of our education services, including guest lecturers, speakers, mentors and events personnel represent true diversity, and that staff and students have an opportunity to suggest developmental training opportunities and events that deepen their sense of belonging and foster inclusivity.

TILEYARD EDUCATION
DATA PROTECTION POLICY AND MANUAL

Policy Owner: Head of Student Services
Last Updated: December 2022
Last Reviewed: December 2022
Next Review Date: December 2023

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

CONTENTS 2

FOREWORD

This Data Protection Manual is the means by which Tileyard Education Ltd trading as Tileyard Education (TYE) 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.

TYE 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.

The TYE Managing Director 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 TYE and, as such, all personnel at every level shall practice the procedures herein established.

DATA PROTECTION POLICY

The Data Protection Act 1998 requires TYE 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 TYE 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
● 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

TYE's designated **Data Controller** is the TYE Managing Director. They exercise the following responsibilities:

● 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 TYE's Data Protection Manual is appropriate for the types of personal data being processed
● Ensuring that TYE maintains an up-to-date notification of its use of personal data with the Information Commissioner's Office.

TYE's designated **Data Protection Officer** is the TYE Managing Director. They are responsible for:

● Training and advising staff on the implementation of TYE Data Protection Manual and GDPR requirements

•Monitoring compliance with TYE'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 TYE

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 TYE in connection with their employment, registration or other contractual agreement is accurate to the best of their knowledge
● Informing TYE 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 TYE details of which will be sent out from time to time, and informing TYE of any errors that need amending
● As a Data Controller, TYE 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, 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.

TYE 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 TYE 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 TYE is collected in order to ensure that TYE 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 TYE in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within TTYE. 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 TYE 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 TYE 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 TYE

Conditions for Processing

At least one of the following conditions must be met whenever TYE 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 TYE 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

TYE 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 TYE will be furnished with a copy of this Data Protection Manual
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE will be made fully aware of both their individual responsibilities and TYE responsibilities under the Act
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE handling personal data will be appropriately trained to do so
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE handling personal data will be regularly evaluated and reviewed
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE 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 TYE arising out of this Data Protection Manual and the Act
● Where any contractor, agent, consultant, partner or other party working on behalf of TYE handling personal data fails in their obligations under this Data Protection Manual that party shall indemnify and hold harmless TYE 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 TYE 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 TYE holds about them. SARs must be made in writing, accompanied by the correct fee; TYE 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 TYE 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 TYE 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

TYE collects employee related personal data in order to ensure that TYE can effectively manage and facilitate efficient transactions with its employees and contractors as well as to comply with relevant employment law. TYE 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 TYE.

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

TYE 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.

TYE 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 TYE (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.

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

Health Records

TYE 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 TYE 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

TYE 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

TYE 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.

TYE will ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE'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, TYE is not bound by the Freedom of Information Act 2000; however, TYE is committed to being open and honest in the conduct of its operations. To this end, TYE 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
DATA PROTECTION POLICY AND MANUAL

Policy Owner: Head of Student Services
Last Updated: December 2022
Last Reviewed: December 2022
Next Review Date: December 2023

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

CONTENTS 2

FOREWORD

This Data Protection Manual is the means by which Tileyard Education Ltd trading as Tileyard Education (TYE) 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.

TYE 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.

The TYE Managing Director 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 TYE and, as such, all personnel at every level shall practice the procedures herein established.

DATA PROTECTION POLICY

The Data Protection Act 1998 requires TYE 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 TYE 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
● 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

TYE's designated **Data Controller** is the TYE Managing Director. They exercise the following responsibilities:

● 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 TYE's Data Protection Manual is appropriate for the types of personal data being processed
● Ensuring that TYE maintains an up-to-date notification of its use of personal data with the Information Commissioner's Office.

TYE's designated **Data Protection Officer** is the TYE Managing Director. They are responsible for:

● Training and advising staff on the implementation of TYE Data Protection Manual and GDPR requirements

•Monitoring compliance with TYE'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 TYE

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 TYE in connection with their employment, registration or other contractual agreement is accurate to the best of their knowledge
● Informing TYE 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 TYE details of which will be sent out from time to time, and informing TYE of any errors that need amending
● As a Data Controller, TYE 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, 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.

TYE 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 TYE 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 TYE is collected in order to ensure that TYE 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 TYE in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within TTYE. 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 TYE 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 TYE 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 TYE

Conditions for Processing

At least one of the following conditions must be met whenever TYE 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 TYE 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

TYE 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 TYE will be furnished with a copy of this Data Protection Manual
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE will be made fully aware of both their individual responsibilities and TYE responsibilities under the Act
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE handling personal data will be appropriately trained to do so
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE handling personal data will be regularly evaluated and reviewed
● All employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE 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 TYE arising out of this Data Protection Manual and the Act
● Where any contractor, agent, consultant, partner or other party working on behalf of TYE handling personal data fails in their obligations under this Data Protection Manual that party shall indemnify and hold harmless TYE 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 TYE 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 TYE holds about them. SARs must be made in writing, accompanied by the correct fee; TYE 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 TYE 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 TYE 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

TYE collects employee related personal data in order to ensure that TYE can effectively manage and facilitate efficient transactions with its employees and contractors as well as to comply with relevant employment law. TYE 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 TYE.

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

TYE 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.

TYE 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 TYE (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.

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

Health Records

TYE 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 TYE 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

TYE 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

TYE 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.

TYE will ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of TYE 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 TYE'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, TYE is not bound by the Freedom of Information Act 2000; however, TYE is committed to being open and honest in the conduct of its operations. To this end, TYE 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
CHILD PROTECTION AND SAFEGUARDING POLICY
Policy Owner: Head of Student Services
Last Updated: December 2022
Last Reviewed: December 2022
Next Review Date: December 2023

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

Key Purpose and Objectives

Tileyard Education has a statutory and moral duty to ensure that it functions with a view to safeguarding and promoting the welfare of young people receiving education and training at Tileyard Education.

This Policy outlines Tileyard Education's procedures for dealing with the protection of children, young people and adults 'at risk'.

It clarifies roles and responsibilities within the organisation and the processes which should be followed to safeguard all learners.

The Islington Safeguarding Children's Board (ISCB) have produced Child Protection Interagency Procedures and Practice Guidelines which Tileyard Education will adopt and will be accessed for advice and guidance https://www.islingtonscb.org.uk

Key Responsibilities

The Managing Director is ultimately responsible for safeguarding issues and compliance, alongside the Director of Education.

The designated senior member of staff with lead responsibility for safeguarding is the Head of Teaching and Learning - Steve Cole.

Other staff with specific responsibility are detailed in the first section.

Policy and Legislative Connections

- The Children Act 1989 places a duty on Local Authorities to take steps to protect children and gives certain powers to the Police so that they may take action to protect children.
- 2004 Children's Act- Every Child Matters placed a duty on schools/services to safeguard and promote the well-being of pupils and introduced Children Services and a Local Safeguarding Children's Board (LSCB).
- Working Together to Safeguard Children September 2018
- Islington Safeguarding Children Board (ISCB)
- Keeping Children Safe in Education September 2019
- The Care Act 2014

OVERVIEW

Scope

The Children Act 1989 defines a **child** as "a person under the age of 18". This could therefore include:

- Any student up to the age of 18;
- Any other person under the age of 18 who becomes known to Tileyard Education, including visitors and staff.

Where reference is made within this policy, to children and young people, this term is used to mean those under the age of 18. Any concerns raised to Local Authority will be raised to Children's Social Care.

The term "adult at risk" is used within this policy in replacement of the term "vulnerable adult".

An adult at risk is a person of 18 years of age or older who is, or may be, in need of community care services by reason of mental or other disability, age or illness; and who is, or may be, unable to take care of him or herself, or be unable to protect him or herself against significant harm or exploitation.

An adult at risk may therefore be a student who, for example:

- Is an older person who is frail due to ill health, physical disability or cognitive impairment;
- Has a learning disability;
- Has a physical disability and/or a sensory impairment;
- Has mental health needs including dementia or a personality disorder;
- Has a long-term illness/condition;
- Misuses substances or alcohol;
- Is a carer such as a family member/friend who provides personal assistance and care to adults and is subject to abuse;
- Lacks the mental capacity to make particular decisions and is in need of care and support.

Key Principles

Children, young people and adults at risk have a fundamental right to be protected from harm. The protection of children and adults at risk is a shared community responsibility. The abuse of children and adults at risk is a clear infringement of human rights and in many cases may be a criminal offence.

Tileyard Education is committed to ensuring that it:

- Creates a positive and safe environment;
- Actively safeguards and promotes the welfare of students, following robust procedures;
- Identifies children, young people and adults 'at risk' who are suffering, or likely to suffer, significant harm;
- Takes appropriate action to see that such children, young people and adults 'at risk' are kept safe, both at home and at Tileyard Education;
- Provides well-trained and well-supported staff to deliver safeguarding provision;
- Adopts an attitude of 'it could happen here'.

All staff will receive training adequate to familiarise them with safeguarding issues and responsibilities and Tileyard Education procedures and policies, with further updates every year. There will be a senior member of the Tileyard Education Executive Management Team overseeing strategic responsibilities and a member of the Senior Management Team with lead responsibility for safeguarding. There will also be identified deputies. These persons will undertake specific high level safeguarding training every 2 years as recommended by the Islington Safeguarding Children Board (ISCB). The Safeguarding Leads will be nominated to liaise with the Local Authority and Director of Education on issues of safeguarding and the CEO in the event of allegations of abuse made against the Director of Education or one of the SafeguardingLeads.

A Safeguarding Working Group and a Safeguarding Review Group will oversee the safeguarding agenda and safeguarding will feed into a number of other meetings and working groups.

RESPONSIBILITY FOR ACTIONS WITHIN THE POLICY

Designated Safeguarding Lead

The designated senior member of staff with lead responsibility for safeguarding is Steve Cole. They have a key duty to take lead responsibility for raising awareness within the staff of issues relating to the welfare of children, young people and adults 'at risk', and the promotion of a safe environment for all students learning at Tileyard Education and is also the Looked After Children (LAC) designate.

The DSL will receive training at least every two years along with training in safeguarding issues and inter-agency working, as required by the Local Safeguarding Partnership. The DSL will also attend the local DSL network to ensure that practices and knowledge are kept up to date with the current local climate and links are created with peers. The DSL will receive Peer Support and supervision from an external party.

Responsibilities of the DSL includes:

- Overseeing the referral of cases of suspected abuse or allegations to Social Care Services.
- Overseeing the referral of cases to 'Channel' where there is a concern of radicalisation.
- Providing advice and support to other staff on issues relating to child and adult safeguarding.
- Ensuring a record of any child and adult protection referrals, complaints or concerns (even where that concern does not lead to a referral) is maintained.
- Ensuring that parents/carers of children and young people within Tileyard Education have access to the Safeguarding Policy.
- Liaising with the Islington Safeguarding Children Board (ISCB) or relevant Local Authority and other appropriate agencies
- Oversee staff acting as a contact point for young people who are 'looked after' or who are 'leaving care'.
- Ensure that all staff receive basic training in safeguarding issues and are aware of Tileyard Education's safeguarding procedures.
- Updating policies when there is a change in policy or requirements locally or nationally.
- Undertaking an annual audit of safeguarding procedures.
- Ensuring that a DSL is on site during all times the setting is open to under 18's.
- Reporting deficiencies in procedure or policy identified by the ISCB (or others) to the Director of Education and/or CEO at the earliest opportunity.
- Convene a review group meeting for all Designated Staff to discuss current cases and to review any applications that pose a safeguarding risk.
- Review Safeguarding Risk Assessments where required.
- Where needed, they may also decline offers for students who pose a safeguarding risk.
- Lead the liaison between Social Care Services and TYE in connection with allegations against staff. This will include undertaking or supporting the investigation and communicating allegations and findings to the Director of Education.

Deputy Safeguarding Lead

The Deputy Safeguarding Lead is Oli Fisher. The Deputy DSL will support the DSL in carrying out their safeguarding role. Some responsibilities may be delegated to the Deputy DSL but the DSL will remain ultimately responsible.

The Deputy DSL will undertake DSL training every two years along with training in safeguarding issues and inter-agency working, as required by the ISCB. The deputy will also receive Peer Support and supervision from an external party.

In addition to supporting the responsibilities outlined in 2.1, the deputy will also:

- Refer cases and support DSO's to refer to social care or other relevant agencies.

- LiaisE with the manager(s) responsible for secondary schools which send pupils to Tileyard Education to ensure that appropriate arrangements are made for their pupils.
- Undertake Safeguarding Risk Assessments where required.
- Ensure all cases are recorded timely and accurately.
- Provide advice and support to DSO's and other staff in the absence of the DSL.

Designated Safeguarding Officers

Tileyard Education has further Designated Staff.

All designated staff will undertake DSL training every two years along with training in safeguarding issues and inter-agency working, as required by the ISCB. All staff dealing with disclosures will receive Peer Support and attend the Safeguarding Review Group meetings.

They are expected, when needed to support all responsibilities outlined in 2.1 and 2.2.

Other Staff Members

All staff, regardless of role, have a responsibility to safeguard our students. There are some key roles/teams however that have a remit to pick up and deal with wider safeguarding issues presented by students/staff.

These staff will:

- Pass on any concerns to the DSL, Deputy or DSO's;
- Know how to make an appropriate referral;
- Be available to provide advice and support to other staff on issues relating to child and adult safeguarding;
- Have a responsibility to be available to listen to students who have concerns;
- Deal with individual cases, including attending case conferences and review meetings as appropriate;
- Receive training in wider safeguarding issues.

For students with Additional Needs who may need advocacy/ support, a member of the Academic Learning Support team will be assigned.

The Director of Education

The Director of Education - Harry Leckstein - is responsible for liaising with the Executive Management Team, Directors and the senior staff members with lead responsibility over matters regarding child protection, including:

- Ensuring that Tileyard Education has adopted the Interagency Procedures produced by thE Islington Safeguarding Children Board (ISCB)
- Ensuring that the senior staff consider and approve the Tileyard Education Child Protection and Safeguarding Policy each year;
- Ensuring that each year the senior staff are informed of how Tileyard Education and its staff have complied with the policy, including a report on the training that staff have undertaken;
- Ensuring there are procedures for reporting and dealing with allegations of abuse against members of staff;
- The safe recruitment of staff;
- Overseeing the liaison between Social Care Services and an independent body in connection with allegations against the Senior Staff Member(s) with Lead Responsibility. This will not involve undertaking any form of investigation, but will ensure good communication between the parties and provide information to assist inquires. For allegations against the Director of Education, the CEO will assume this responsibility.

To assist in these duties, the Director of Education shall receive appropriate training as directed by ISCB.

Independent Body Acting as HR

The designated Independent Body has responsibility for

- Ensuring that appropriate training has taken place for all staff and is made available for volunteers, including the logging that all staff have read Part one of Keeping Children Safe in Education (See gobo/policies and procedures/safeguarding).
- Ensuring that there are safe recruitment policies and practices, including enhanced Disclosure and Barring Service (DBS) checks on staff who have regular, unsupervised access to children up to age 18 and Vulnerable Adults and where appropriate, for governors and volunteers.
- Ensuring that there is record of all DBS checks undertaken on staff and where, appropriate, governors and volunteers.
- Ensuring that there is a robust procedure for responding to concerns and allegations of abuse regarding employees who work with children and young people, including a clear and robust 'whistle-blowing' policy.
- Manage the process of allegations against staff alongside the DSL and external agencies (where required).

The above responsibilities may be delegated, where appropriate, but the designated Independent Body maintains responsibility.

The Work Placement Co-ordinator

The Work Placement Co-ordinator (WPC) will take responsibility for students that are out on placement with support and advice from the DSL. The WPC will liaise with employers regarding any concerns and will report them to the safeguarding team.

The WPC will also take responsibility for ensuring any DBS checks are carried out (where needed) and any self-disclosure forms with employers.

The WPC will ensure that employers are aware of their safeguarding responsibilities and will report any concerns to the DSL. The WPC will also ensure that all employers receive the safeguarding expectations document.

TYPES OF ABUSE

Children and Young People under 18

Tileyard Education recognises the following as definitions of abuse and neglect as defined within *Keeping Children Safe in Education:*

Abuse: a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. They may be abused by an adult or adults or another child or children, this could include their peers within Tileyard Education.

Keeping Children Safe in Education outlines four areas of abuse as follows:

Physical abuse: a form of abuse which may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately 2.induces, illness in a child.

Emotional abuse: the persistent emotional ill treatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve conveying to children that they are worthless or unloved, inadequate, or valued only in so far as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond the child's developmental capability as well as overprotection and limitation of exploration and learning, or preventing the child participating in normal social interactions. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyber-bullying) causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some

level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

Neglect: the persistent failure to meet a child's basic physical/and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to: provide adequate food, clothing and shelter (including exclusion from home or abandonment); protect a child from physical and emotional harm or danger; ensure adequate supervision (including the use of inadequate care-givers); ensure access to appropriate medical care or treatment. It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

In addition, Keeping Children Safe in Education identifies that there are wider safeguarding issues that we need to consider and act upon. Some of these include:

Child Sexual Exploitation
Bullying including Cyberbullying
Domestic Violence
Drugs and Alcohol Misuse
Peer on Peer Abuse (3.4)
Fabricated or Induced Illness
Faith Abuse
Honor Based Violence
Female Genital Mutilation (FGM) (see 3.2)
Forced Marriage
Gangs and Youth Violence
Gender-based Violence
Private Fostering
Mental Health
Preventing Radicalisation *(see 3.3)*
Sexting
Relationship Abuse
Children Missing Education

Children Missing from Home or Care
Trafficking
Hate Crime
Missing Children and Adults
Serious Violence
Contextual Safeguarding
Suicidal ideation/Attempts

Female Genital Mutilation: Female Genital Mutilation (FGM) comprises all procedures involving partial or total removal of the external female genitalia or other injury to the female genital organs. It is illegal in the UK and a form of child abuse with long-lasting harmful consequences. Professionals in all agencies, and individuals and groups in relevant communities, need to be alert to the possibility of a girl being at risk of FGM, or already having suffered FGM.

Tileyard Education recognises that it now has a statutory duty, to report to the police any discovery that FGM appears to have been carried out on a girl under 18. Those failing to report such cases will face disciplinary sanctions. Any suspected cases of FGM should be reported to one of Tileyard Education's Designated Safeguarding Officers who will involve Social Care as appropriate.

Preventing Radicalisation: Protecting individuals from the risk of radicalisation should be seen as part of Tileyard Education's wider safeguarding duties, and is similar in nature to protecting individuals from other forms of harm and abuse. During the process of radicalisation, it is possible to intervene to prevent vulnerable people being radicalised.

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. As with managing other safeguarding risks, staff should be alert to changes in individual's behaviour which could indicate that they may be in need of help or protection. Staff should use their professional judgement in identifying individuals who might be at risk of radicalisation and refer any concerns to one of Tileyard Education's Designated Safeguarding Staff.

Tileyard Education recognises that is now has a statutory duty to have 'due regard to the need to prevent people from being drawn into terrorism. In complying with the duty, Tileyard Education commits to demonstrating an awareness and understanding of the risk of radicalisation and extremism in their institution. Tileyard Education has produced an action plan that considers levels of risk in the key areas as outlined by the Department of Education.

Prevent at Tileyard Education, falls under the banner of safeguarding and will be led by the Head of Teaching and Learning - Steve Cole - who is also the Designated Safeguarding Lead. If any staff have any concerns relating to students and radicalisation, they should refer them to one of Tileyard Education's Designated Safeguarding Staff. Tileyard Education's Designated

Safeguarding Staff will then work with external agencies such as Channel or the regions local Prevent Co-ordinator if appropriate.

Peer on Peer Abuse: Peer on Peer abuse is a specific form of abuse that is a particularly challenging and complex area of safeguarding. Staff should recognise that students are capable of abusing their peers and inappropriate behaviour should not be tolerated or dismissed as 'banter'.

Peer in Peer abuse should be referred to the disciplinary process and reported as a safeguarding issue.

Types of Peer on Peer abuse can include:

- Physical abuse such as biting, hitting, hair pulling.
- Sexually harmful behaviour such as touching, assault, inappropriate and unwanted Touching.
- Bullying and cyber bullying.
- Sexting.
- Abuse in relationships.

Adults at risk aged 18+: Chapter 14 within the Care Act 2014 replaces the 'No Secrets' guidance The safeguarding duties within the Care Act apply to an adult who:

- Has needs for care and support (whether or not the local authority is meeting any of those needs) and;
- Is experiencing, or at risk of, abuse or neglect and;
- As a result of those care and support needs is unable to protect themselves from either the risk of, or the experience of abuse or neglect.

Islington Adult Safeguarding Board (IASB) now refers to adults to whom the duty applies as 'adults at risk'.

Tileyard Education recognises the following as definitions of abuse and neglect as defined within *Chapter 14 -'The Care Act'*

Physical abuse: this includes assault, hitting, slapping, pushing, misuse of medication, restraint or inappropriate physical sanctions.

Domestic violence: this includes psychological, physical, sexual, financial, emotional abuse; so called 'honour' based violence.

Sexual abuse: this includes rape, indecent exposure, sexual harassment, inappropriate looking or touching, sexual teasing or innuendo, sexual photography, subjection to pornography or witnessing sexual acts, indecent exposure and sexual assault or sexual acts to which the adult has not consented or was pressured into consenting.

Psychological abuse: this includes emotional abuse, threats of harm or abandonment, deprivation of contact, humiliation, blaming, controlling, intimidation, coercion, harassment, verbal abuse, cyber bullying, isolation or unreasonable and unjustified withdrawal of services or supportive networks.

Financial or material abuse: this includes theft, fraud, internet scamming, coercion in relation to an adult's financial affairs or arrangements, including in connection with wills, property, inheritance or financial transactions, or the misuse or misappropriation of property, possessions or benefits.

Modern slavery: this encompasses slavery, human trafficking, forced labour and domestic servitude. Traffickers and slave masters use whatever means they have at their disposal to coerce, deceive and force individuals into a life of abuse, servitude and inhumane treatment.

Discriminatory abuse: this includes forms of harassment, slurs or similar treatment; because of race, gender and gender identity, age, disability, sexual orientation or religion.

Organisational abuse: this includes neglect and poor care practice within an institution or specific care setting such as a hospital or care home, for example, or in relation to care provided in one's own home. This may range from one off incidents to on-going ill-treatment. It can be through neglect or poor professional practice as a result of the structure, policies, processes and practices within an organisation.

Neglect and acts of omission: this includes ignoring medical, emotional or physical care needs, failure to provide access to appropriate health, care and support or educational services, the withholding of the necessities of life, such as medication, adequate nutrition and heating.

Self-neglect: this covers a wide range of behaviour neglecting to care for one's personal hygiene, health or surroundings and includes behaviour such as hoarding.

INFORMATION SHARING AND CONFIDENTIALITY

Sharing Information

Information sharing is vital to safeguarding and promoting the welfare of children, young people and adults at risk.

Where there are concerns about the safety of a child, young person or an adult at risk, the sharing of information in a timely and effective manner between organisations can reduce the risk of harm. Whilst the Data Protection Act 1998 places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing

information where the failure to do so would result in a child, young person or adult at risk being placed at risk of harm.

Staff should use their judgement when making decisions on what information to share and when. A flowchart on when and how to share information is available in Appendix 3. If any member of staff is in doubt, they should contact one of the Designated Safeguarding Staff.

The principles of sharing information.

Tileyard Education adopts the 'seven golden rules to sharing information' as outlined in the HM Government document '***Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers'.***

Necessary and proportionate – when taking decisions about what information to share, you should consider how much information you need to release. The Data Protection Act requires you to consider the impact of disclosing information on the information subject and any third parties. Any information must be proportionate to the need and level of risk.

Relevant – only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make sound decisions.

Adequate – information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate – information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely – information should be shared in a timely fashion to reduce the risk of harm. Timeliness is a key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm a child, young person or adult at risk.

Secure – wherever possible, information should be shared in an appropriate, secure way.

Record – information sharing decisions should be recorded whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester of the information.

DEALING WITH DISCLOSURES OF ABUSE AND REPORTING CONCERNS

Disclosures

If a member of staff suspects or receives information, or an individual discloses that they are at risk of harm or abuse may be occurring, they have a responsibility to refer to one of the Designated Safeguarding Staff. The safety and welfare of the individual is the primary objective and a member of staff should not delay in seeking medical help in an emergency situation or in contacting other staff to assist if immediate protection is needed.

The member of staff should contact the Head of Teaching and Learning - Steve Cole or the Head of Student Services- Oli Fisher Members of staff should be aware that their duty to refer such suspicions or allegations overrides the concept of confidentiality and this should be explained to the student in a manner best suited to the individual student. Help to communicate with Students with Learning Difficulties / Disabilities will be sought from the Additional Learning Support Manager, if needed.

Procedure for referral

Any allegation, disclosure or suspicion of abuse needs to be taken seriously and handled in a sensitive manner. Individual members of staff should never deal with disclosures in isolation, and **should always refer to a Designated Person**, who will undertake the interview. Information should be strictly limited to those who need to know.

However, as outlined in Part One of Keeping Children Safe in Education **'Where a child is suffering, or is likely to suffer from harm, it is important that a referral to children's social care (and if appropriate the police) is made immediately.'**

Staff should **ALWAYS** make it clear to a young person that they cannot make guarantees of confidentiality. If possible, they should warn the individual about this ***before*** they are given an opportunity to disclose.

If the young person does not wish to continue:

- Encourage them to access support services within Tileyard Education;
- State that you may have to pass on any disclosure
- If the young person wishes to continue:
- Listen carefully to what is being said;
- Keep questions to a minimum, just to clarify what is being said;
- Avoid leading questions, prompting or making comments;
- Suspend your own judgement and remember that you are not investigating the matter;
- Staff should support the student and give reassurances whilst explaining which other people will need to know about the allegations;
- Inform the young person of the actions that will follow your conversation and assure them that they will be kept informed of all developments;

- Staff should make notes of the conversations which may be needed by the investigating agency (e.g. Social Services)

Where possible, staff should include the following:

- Names of those present during the disclosure/allegation
- Address and contact of young person
- Date of birth
- Ethnic origin
- Other agencies already involved
- Date and time of the conversation
- Place where the alleged abuse happened
- Brief description of the allegation
- Any visible injuries
- Any alleged injuries
- Young person's preferred action
- Means of contacting the young person
- Next steps and follow up agreed

Staff should contact one of the Designated Safeguarding Staff immediately after the initial disclosure and pass all information to them. The Designated Safeguarding person who receives the information will make a decision with the SSM about who to contact, usually Social Care and / or the Police.

Appendix 2 provides a flowchart that details how to deal with concerns, suspicions or disclosures of harm or abuse.

Designated Staff Duties

If the student wants to take the allegation forward themselves, the Designated Person should support the student in contacting Social Care Services, and ensure that is made within 24 hours of initial disclosure/allegation. (The police may be contacted if the student is in immediate danger of harm to self or others).

If the Designated Person decides that they must report the allegation, the Designated Person should contact Social Services by telephone and complete any additional paperwork within 24 hours of the initial disclosure/allegation, if requested. If a Designated Person is unsure whether to make a referral, they should contact the Islington Safeguarding 02075272299.

The student and referring staff member should be informed of the action being taken and the reasons for this decision. This should happen before Social Care Services are informed, unless doing so would place the person at greater risk. In this case, both staff and student should be contacted as soon as safety considerations of the person permit.

The parents/carer for a child, young person or adult at risk should also be informed of the action being taken, unless doing so would place the person at greater risk.

The Designated Person should contact Social Care Services by telephone, in the first instance. The date and time of the contact and the duty officer's name should be recorded.

Where any proceedings follow the initial referral, the Designated Person should provide relevant feedback to the student as recommended by Social Services.

The Designated Person should ensure that all written records relating to the incident are kept indefinitely, in a secure location. The Designated Person is responsible for ensure that cases are fully recorded and updated. All cases should remain on review until concluded. If a suitable intervention is not received from Social Care, the DSL should support the DSO to escalate the concerns with social care – team manager, service manager, head of service, director of safeguarding, Safeguarding Children's Partnership chair.

Designated staff should, at all times, keep the DSL up to date on proceedings.

Procedure for post-18's

It is **not** a legal requirement to inform statutory agencies of abuse cases involving students over 18 years old who aren't deemed to be adults at risk. However, if someone at Tileyard Education is over 18 and disclose information regarding anyone under 18 who they may be associated with, e.g. their own children, siblings, other family members, then you must report this to one of the Designated Safeguarding Staff.

A duty of care is maintained for students over 18 and support/referrals will be offered.

REPORTING AND DEALING WITH ALEEGATIONS OF ABUSE AGAINST MEMBERS OF STAFF

Introduction

In rare instances, staff of education institutions have been found responsible for child abuse. Because of their frequent contact with children and young people, staff may have allegations of child abuse made against them. Tileyard Education recognises that an allegation of child abuse made against a member of staff may be made for a variety of reasons and that the facts of the allegation may or may not be true. It is imperative that those dealing with an allegation maintain an open mind and that investigations are thorough and not subject to delay.

Tileyard Education recognises that the Children's Act 1989 states that the welfare of the child is the paramount concern. It is also recognised that hasty or ill-informed decisions in connection with a member of staff can irreparably damage an individual's reputation,

confidence and career. Therefore, those dealing with such allegations within Tileyard Education will do so with sensitivity and will act in a careful, measured way.

Receiving an Allegation from a Child, Young Person 16-18 or Vulnerable Adult

A member of staff who receives an allegation about another member of staff from a child/young person should follow the guidelines in Section 3 for dealing with disclosure.

The **Procedure for dealing with allegations of abuse against members of staff** (see Appendix 5) should be followed.

Allegations may be received via the complaints process, the DSL will lead on the complaint with Independent HR body.

Appendix 1

Safeguarding Working Group

Tileyard Education is committed to the safeguarding of all staff and students and recognises it has a duty of care to protect children and adults 'at risk' from maltreatment; prevent impairment of their health and development; ensure that they live in circumstances consistent with the provision of safe and effective care; and take action to enable all children and adults 'at risk' have the best outcomes.

It is within the duty of care to act if there is a cause for concern and to notify the appropriate agencies so that the matter can be investigated and further action be taken if necessary. Tileyard Education has a responsibility to provide information to other appropriate agencies in response to safeguarding matters.

As part of Tileyard Education's responsibilities, it convenes a Safeguarding Working Group to oversee all aspects of Safeguarding. The group will have the following responsibilities:

- Ensure that Tileyard Education fulfils its role in relation to safeguarding children and adults 'at risk' and has the required procedures in place.
- Review and advise on the implementation of all related safeguarding legislation.
- Establish and maintain policies and procedures relating to safeguarding including practices around 'Safer Recruitment'.
- Ensure staff are appropriately trained in accordance with the Islington Safeguarding Children Board (ICSB).
- Agree and support procedures that enable risk assessments to be carried out on potential students who may pose a threat to others and / or themselves.
- Contribute towards providing an environment that is healthy, safe and secure including making recommendations on site security.
- Work in conjunction with Health & Safety, to triangulate common themes and concerns.
- Share information relating to safeguarding and compliance issues.
- Feed issues into other teams / departments internally or externally, as part of development and improvement plans.

MEMBERSHIP

The Safeguarding Working Group will be chaired and convened by the Designated Safeguarding Lead. Membership of the group will include:

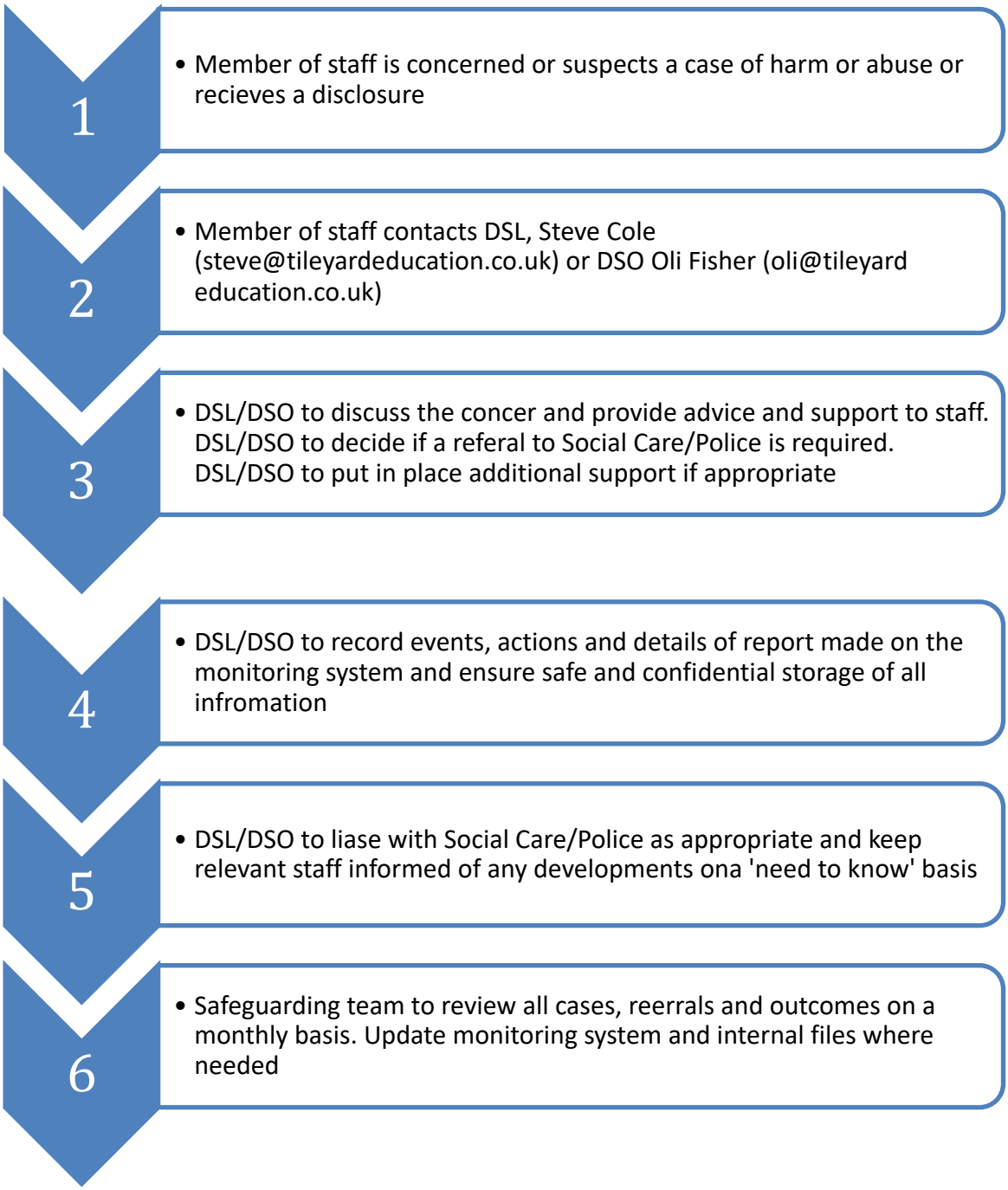
Title	Name
Managing Director	Harry Leckstein

Operations manger	Ciaran Robinson
Head of Teaching and Learning	Steve Cole
Head of Student Services	Oli Fisher
Head of A&R and Commercial Partnerships	Jamie Searls

The meetings will be held termly, with agenda items being tabled on a meeting by meeting basis.

Appendix 2

Flowchart for dealing with concerns, suspicions or disclosures of harm or abuse



Appendix 3

For use by the Safeguarding Team

ISCB

Children's Social Care	**Adult Social Care**
Within office Hours: (Mon - Thurs 8.30a.m. - 5.00 p.m. Fri 8.30am – 4.30pm) - 02075274234 **Outside Office Hours (including weekends & bank holidays):** Emergency Duty Team: 02072260992	**Office hours: Monday – Thursday 8.30am to 5.00pm, Friday 8.30am to 4.30pm** **Access Duty Team for Adults –** 02075272299 **Outside Office Hours (including weekends & bank holidays):** 02072260992

Appendix 4

Dealing with Allegations Against Staff

1. Action to be taken pre-employment

Where a candidate has applied to volunteer or for work and appears on the Disclosure and Barring Service (DBS) barred list, or there are serious concerns about an applicant's suitability to work with Children and Adults at Risk, Tileyard Education has a duty to notify the DBS.

Referral information is found at point 4.

2. Action to be taken in employment

Responding to an allegation of abuse against a staff member

Where allegations indicate that an employee may be unsuitable to continue to work with Children or an Adult at Risk in either their present position or any capacity as they may have:

- Behaved in way that has harmed a child or an adult at risk or may have harmed a child or an adult at risk.
- Possibly committed a criminal office against or related to a child or an adult at risk.
- Behaved toward a child, children or an adult(s) at risk in a way that indicates that they may pose a risk of harm to them.

Note:
The concept of 'harm' may have occurred in either a personal or professional capacity

The following action must be taken:

The allegation must be raised with the Head of Teaching and Learning - Steve Cole, or where they are the subject of the allegation, the Director of Education - Harry Leckstein- should be contacted.

The Head of Teaching and Learning - Steve Cole,will then, with support from suitably experienced and senior Tileyard Education personnel, immediately discuss the allegation with the Local Authority Designated Officer(s).

The purpose of this discussion is to consider the nature, content and context of the allegation and agree a course of action. This could include a decision that no further action is to be taken.

In these cases this decision and a justification for it will be recorded and the Tileyard Education, together with the Local Authority Designated Officer, will agree what information should be put in writing to the individual concerned and by whom.

The Local Authority Designated Officer is always contacted before any action is taken in respect of a staff member unless there is an immediate risk to others or evidence of a criminal offence when the police may be contacted.

Tileyard Education will act on the advice of the Local Authority Designated Officer. In Islington, the Designated Officer role is undertaken by the following people:

Name	Role	Contact Details
Timur Djavit	LADO	02075278102 LADO@islington.gov.uk

Having obtained advice from the LADO Timur Djavit, Tileyard Education will usually inform the employee about the allegations. Where the employee is a union member, they will be advised to seek the support of that body from the outset.

The employee will be provided with as much information as possible, however where a strategy discussion is required, or other services need to be involved, Tileyard Education may not be able to disclose information until all agencies have agreed what can be disclosed.

Where allegations indicate that another person is or has been at risk of harm, or the allegation warrants investigation by the police / social services, or where the alleged act may constitute serious or gross misconduct, the employee should be suspended on full pay for good and urgent cause. Other reasonable alternatives will be considered prior to suspension.

Details on suspension arrangements are found within the Staff disciplinary policy. The member of staff is suspended to enable an investigation to be carried out and it does not infer that any conclusions have been reached about the validity of the allegation.

If immediate suspension is considered necessary, the rationale and course of action should be agreed with the Director of Education - Harry Leckstein. This should also include what alternatives to suspension were considered and why they were rejected.

An investigation will then be carried out following the process outlined in the Disciplinary policy. It does not automatically follow that the outcome is a Disciplinary penalty, but this policy provides the framework for the process to be followed.

Head of Teaching and Learning- Steve Cole will assume responsibility under the direction of the Director of Education and CEO, for the investigation into the allegations and for ensuring

that the employee is kept informed of progress, adhering to the guidelines contained in the document 'Keeping Children Safe in Education 2019'.

Head of Teaching and Learning - Steve Cole will assume responsibility under the direction of the Director of Education and CEO for ensuring that parents and carers of those 'at risk' involved in the allegation are kept informed upon the advice of the Director of Education / Local Authority Designated Officer.

If an employee tenders their resignation in response to an allegation, a full investigation will still be undertaken. Every effort should be made to fully investigate the allegation and come to a conclusion, even if the employee refuses to co-operate with the process. Where this is the case it should be noted.

Settlement agreements will never be used in situations where an allegation of this nature has been received.

The investigation report, all statements taken (signed) and all associated documents will be provided to Head of Teaching and Learning - Steve Cole who will liaise with Director of Education, CEO to determine the next steps.

3. Action to be taken to report misconduct post employment

Where Tileyard Education has ceased to employ someone engaged in Regulated Activity because they were considered unsuitable to work with children or adults at risk (Safeguarding reasons) a referral will be made to the Disclosure and Barring Service promptly and within 1 month of the employment ending. This includes situations where the employee would have been dismissed had they not resigned.

Details of the information required for a referral is found on the forms below.

Historical allegations against a member of staff who is no longer employed will be referred to the Police.

4. Referral information

Referrals should be made to: Disclosure and Barring Service PO Box 181 Darlington DL1 9FA

5. General Principles

Tileyard Education recognises that it has a duty of care to employees and as such will provide support for anyone facing an allegation. Should suspension be required they will be provided with a named contact within Tileyard Education.

All efforts will be made to deal with allegations of abuse as quickly, fairly and consistently as possible and in a way that complies with procedural requirements, the effective protection of the child or adult at risk and at the same time supports the employee who is the subject of the allegation.

6. Record keeping

Details of allegations which have been found to be malicious will be removed from the employee's record.

For all other allegations Keeping Children Safe in Education requires that a clear and comprehensive summary of the allegation, the details of how the allegation was followed up and resolved, a note of action taken and decisions reached shall be kept on the employee's confidential file with a copy provided to the person concerned.

These records will be retained until either the person has reached the age of 65 or a period of 10 years from the date of the allegation (whichever is longer). This is necessary should any further allegations arise in the future.

7. Employment references

Cases in which an allegation was proven to be false, malicious or unsubstantiated will not be included in an employment reference, regardless of the allegation being a one-off or there being a history of such allegations.

TILEYARD EDUCATION
E-SAFETY POLICY AND PROCEDURES
Policy Owner: Head of Student Services
Last Updated: December 2022
Last Reviewed: December 2022
Next Review Date: December 2023

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

AIM AND SCOPE

TILEYARD EDUCATION (TYE) E-Safety policy and procedures apply to all staff, contractors, tutors, volunteers, trustees, children, young people and anyone working on behalf of TYE.

The aim of the policy is to:

● Protect children and young people who receive TYE'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 TYE.
● Provide staff and volunteers with the principles that guide TYE's approach to E-Safety.
● Protect professionals.
● Ensure that, as an organisation, TYE 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 TYE's Safeguarding and Child Protection Policy.

TYE 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).

TYE 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 or using TYE'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.

TYE will handle complaints regarding E-Safety by taking all reasonable precautions to ensure E-Safety and 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 TYE'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

E-SAFETY OFFICER

Harry Leckstein (harry@tileyard.co.uk / tel +44 (0)7796 950 406)

The responsibility of this role is 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.

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 information/ advice

Contact Unsuitable contact from another user	Tracking Harvesting Publishing information about themselves	Being bullied, harassed, stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
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

VULNERABILITY OF CERTAIN GROUPS

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-practiceguidance/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.

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; 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

TYE 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 TYEwill ensure that the evidence is preserved.

TYE 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.

ACCEPTABLE USE POLICY (AUP)

TYE's AUP clearly identifies the expectations and boundaries for the use of technology both provided by TYE 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.

TYE Staff/volunteers and users should be aware of the potential consequences of any breach of the AUP.

TYE 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.

● TYE staff/volunteers will receive training that includes how to differentiate between their personal and professional behaviour especially when they are online.
● TYE 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 TYE'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 TYE's ICT must sign an AUP contract.

For 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 TYE including email, internet, intranet, network resources, software, equipment and systems.

I will only use TYE'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 TYE systems.

I will ensure all documents, data, etc are saved, accessed and deleted in accordance with TYE'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 TYE.

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 TYE is provided solely for professional use

I will access TYE'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 TYE's data security protocols when using confidential data at any location.

Any information seen by me with regard to service users held within TYE 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 TYE'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 TYE including email, internet and equipment ("ICT").

I will use TYE'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.

TYE 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 Harry Leckstein or Trustee responsible for E-Safety

I will not use TYE'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 TYE I will follow the rules set out in this agreement, in the same way as if I was using TYE'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

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

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, knowingl 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

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

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT