e-Safety / Acceptable Use / ICT Policy

This policy MUST be read in conjunction with the Safeguarding Policies

Thomas Keaney, CEO and Schools' Proprietor

Date of next formal review, June 2019

This policy applies to all TCES Group schools and services

Essex Fresh Start Independent School

East London Independent School

North West London Independent School

Create Service Personalised Therapeutic Education

Contents

Guidance for Reader

Policy Review
This policy is reviewed on an annual basis by the School Senior Management Team and the company Management Development Group (Company's Head teacher and SLT members) and is signed off accordingly by the School Proprietor (recorded and indicated as per the back page of this policy – **The TCES Group Policy Sign off**.)

Policy Conjunction
It is important to note that this 'e-Safety/acceptable use/ICT' policy embodies the philosophy and ethos of the TCES Group, and applies to all school staff (including staff, pupils/pupils, volunteers, parents /carers, visitors, community users) who have access to and are users of School ICT systems, both on-site and off-site.

Policy Legislation
The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of School, but is linked to the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the School

Policy Availability
The e-Safety/Acceptable Use/ICT Policy is available in hard copy in our Policies and Procedures folder in each administrator's office and every member of staff, parent and child will be required to sign an AUP (Acceptable Use Policy) Agreement

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- set out the key principles expected of all members of the School community with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff at School
- assist School staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other School policies.
- ensure that all members of the School community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our School communities can be summarised as follows:

Content

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

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

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

Role	Key Responsibilities
Head teacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the School uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant in conjunction with the training coordinator • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures

Group Training and Quality Assurance Safeguarding Manager
 	
Facilities at Central Services
	• Take day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the School e-safety documents
	• To promote an awareness and commitment to e-safety throughout the School communities
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• To facilitate annual **'intermediate'** training and advice for all staff
	• To be regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	• Educating Parents and raising awareness

School Proprietor	• To ensure that the School follows all current e-Safety advice to keep the children and staff safe • To approve the e-Safety/Acceptable Use/ICT Policy and review the effectiveness of the policy. This will be carried out by the Management Development Group. Receiving regular information about e-safety incidents and monitoring reports. • To support School in encouraging parents and the wider community to become engaged in e-safety activities • Regular reviews with the Group Training and Quality Assurance Safeguarding Manager
Responsible Person	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the Group Training and Quality Assurance Safeguarding Manager regularly • To ensure that e-safety education is embedded across the curriculum

Role	Key Responsibilities
	• To ensure that all data held on pupils on the LEARNING PLATFORM (GOL) is adequately protected
ONSEM (external ICT for schools) Ingenious (ICT for CS staff and encryption of all mobile phones)	• To report any e-Safety related issues that arises, to the Group Training and Quality Assurance Safeguarding Manager and/or facilities department • To ensure that users may only access the School's networks through an authorised and properly enforced password protection, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the School ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on School-owned devices • To ensure that the School's web filtering is applied and updated on a regular basis • To ensure that the use of the network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Group Training and Quality Assurance Safeguarding Manager /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the School's e-security and technical procedures • To ensure that all data held on pupils on the School office machines have appropriate access controls in place • *Impero Education Pro website filtering software currently used alongside LGFL .* (London Grid for Learning) to further strengthen our internet security. This includes a dedicated monitored broadband line and ISP (internet service provider)
Teachers	• To embed e-safety issues in all aspects of the curriculum and other School activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended School activities if relevant) • All online curriculum should be delivered only in the ICT Suite and individual children's password ONLY to be used to log on • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To have signed and understood the staff AUP
All staff	• To read, understand and help promote the TCES Group e-Safety policies and guidance • To read, understand, sign and adhere to the School staff Acceptable Use Agreement

Role	Key Responsibilities
	• To be aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current School policies with regard to these devices • To report any suspected misuse or problem to the Group Training and Quality Assurance Safeguarding Manager or facilities department • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through School based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• To read, understand, sign and adhere to the Pupil Acceptable Use Policy. To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand School guidance on the use of mobile phones, digital cameras and hand-held devices. • To know and understand the policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of School and realise that the e-Safety Policy covers their actions out of School, if related to School • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in School and at home • to help the School in the creation/ review of e-safety policies
Parents/ carers	• To sign up to the TCES Parental Charter • To support the School in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the School's use of photographic and video images • To read, understand and promote the School Pupil Acceptable Use Agreement with their children • To consult with the School if they have any concerns about their children's use of technology
External groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within the School

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be part of School induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole School community, usually on entry to School
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The School will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a School computer or mobile device. Neither the School nor the Local Authority/County Council can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by teacher or Head teacher
  - informing parents or carers
  - removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
  - referral to LA / Police.

The Proprietor and/or Company Complaints Lead is the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher and School Proprietor.
Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
Complaints related to child protection are dealt with in accordance with School child protection procedures.

Review and Monitoring

- TCES has a Group Training and Quality Assurance Safeguarding Manager who will be responsible for document ownership, review and updates
- The e-safety/acceptable use/ICT policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within School
- The e-safety/acceptable use/ICT policy has been written by the TCES Group Training and Quality Assurance Safeguarding Manager and is current and appropriate for its intended audience and purpose
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Management Development Group and other stakeholders. All amendments to the TCES Group e-Safety/Acceptable Use/ICT policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-Safety curriculum

School

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum.
- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons
- to understand the impact of cyber-bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including cyber-bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button (available on our website)
- to understand issues around plagiarism when copying materials from the web, how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- to understand issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling

- Staff to:
  - plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
  - remind pupils about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the School will be displayed when a student logs on to the School network
  - model safe and responsible behaviour in their own use of technology during lessons.

Staff and School Proprietor training

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues
- Provides as part of the induction process, all new staff [including temporary staff with information and guidance on the e-Safety / Acceptable Use/ ICT Policy.

Parent awareness and training

School

- Runs a rolling programme of advice, guidance and training for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets
- Monthly newsletter
- Up to date parent/carer webpage on website
- demonstrations, practical sessions held at School;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

School all users:

- Are responsible for using the School ICT systems in accordance with the relevant e-safety/Acceptable Use / ICT Policy which they will be expected to sign before being given access to School systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
  Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of School and realise that the School's E-Safety Acceptable Use / ICT policy covers their actions out of School, if related to their membership of School
- Will be expected to know and understand School policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand School policies on the taking / use of images and on cyber-bullying

Staff:

- Are responsible for reading the TCES Group e-safety/acceptable use/ICT policy and using the School ICT systems accordingly, including the use of mobile phones, and hand-held devices.

Pupils:

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the School
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In School:

- There is strict monitoring and application of the e-safety/acceptable use/ICT policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the School's escalation processes.

- Support is actively sought from other agencies as needed (eg Safeguarding, CEOP in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contribute to developments within the policy and practice in e-safety within School. The records are reviewed/audited and reported to the School's SLT and School Proprietor
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4 Principles for the use of social media

School Staff must act in the best interests of pupils when creating, participating in or contributing content to social media sites.

In addition staff must:

- Be aware at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- Be accurate, fair and transparent when creating or altering online sources of information on behalf of the school.
- Not engage in activities involving social media that might bring the school into disrepute or represent your views as those of the school.
- Not discuss on social media personal information about pupils/students, the school staff or other professionals you interact with as part of your job.
- Not use social media to attack, insult, abuse or defame pupils/students, their families, colleagues, other professionals, other organisations or the school.

Personal use of social media

In order to safeguard your reputation and the reputation of the School, you are required to follow these guidelines in your personal use of social media.

- You must not have contact through any personal social media with any student or members of their family, from this or any other school, unless the pupil/students are family members.
- You must decline 'friend requests' from pupils/students that you receive to your personal social media accounts. If you receive requests from pupils/students who are not family members, you should discuss these in general terms in class and encourage pupils/students to become 'friends' of the official school site.
- Information that you have access to as part of your employment, including personal information about pupils/students and their family members, must not be discussed on your personal social media.
- Photographs, videos or any other types of images of pupils/students and their families must not be published on your personal social media.
- School email addresses must not be used for setting up personal social media accounts or to communicate through such media.

Guidance for your own privacy and safety

- You are advised to set the privacy levels of your personal accounts as strictly as you can and opt out of public listings on social networking sites.
- You should keep your passwords confidential and change them frequently.
- You should be careful about what you post online; it is not advisable to reveal home addresses, telephone numbers and other personal information.

5 Prevent Duty - Anti-Radicalisation and Extremism

School has a vital role to play in protecting pupils from the risks of extremism and radicalisation. Keeping pupils safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse. If you have a concern for the safety of a specific pupil at risk of radicalisation please follow the 'reporting flowchart' in this policy.

Please see safeguarding policy for full information on Prevent Duty

6. Data security: Management Information System access and Data transfer

The nature of the work at TCES means we have to be extra vigilant with regard to looking after electronic files. In order to comply with GDPR and to safeguard confidential materials, the following must be adhered to:

Password policy

The password you use to log on to your account should be a combination of numbers, letters (capital and lower-case) and symbols. Sharing your password with another person is a violation of this policy. In exceptional circumstances you may need to let someone else know your password to access files on your PC. In this instance, your password must be changed immediately afterwards. It is good practise to regularly change your password, however you should avoid using sequential passwords e.g. password1, password2 etc.

File storage and sharing

For most data storage, files should be saved on your shared or personal drive which is located on a secure server. If you need to share large files with people outside the organisation, please do not use any PII in the subject heading. All data will be encrypted automatically by the encrypted system currently in place.

Removable Media & Portable Storage

This covers items such as USB flash drives, portable hard drives and CD/DVDs. Confidential or pupil information should never be stored on these devices unless all PII (see below) has been removed from any documentation OR the data is encrypted.

Under no circumstances should USBs be used or bought into the company to save data or transfer data. (*exceptation to this is the downloading of CCTV footage for specific reasons which include 'evidence for police when a criminal activity has taken place or when a DSL needs to retain CCTV for an ongoing investigation)*

Personally, Identifiable Information (PII)

Where practical, any documentation shared outside of the TCES group, including via e-mail, should be free of any information which would help identify pupils and staff at School. First-names, initials or anonymous references e.g. “Pupil at (initials of school) ” should be used when discussing pupil affairs. Only disclose as much PII as is necessary in the context of the communication.

File naming

Electronic files should never be saved using any PII, for example “John_Smith_attendance.doc”. This is equally important when saving photographs. Please use either initials or first names if a name is required at all.

External E-mail accounts

All staff, including Integration and agency staff will be provided with a @tces.org.uk account which will be requested on your behalf from the Facilities department at the earliest opportunity.

This must be the only account used for work-related communication. Staff must not forward work emails from their TCES account to a personal / home email account.

Staff are NOT permitted to use their home computer for use of their TCES email account but can use a company provided laptop. All work completed at home must be on a company provided laptop which will have the same encryption system as on all company PCs.

Skyguard

Skyguard is a personal ‘Lone Worker’ alarm system that is provided to staff who work Off-Site with our pupils. Staff should not share this alarm with any other staff member and should ensure that all data has been removed when leaving TCES employment

The General Data Protection Regulations (GDPR)

On 25 May 2018 GPRD effectively replaced the Data Protection Act 1998. The Guide to GDPR can be found at: *https://ico.org.uk/for-organisations/guide-to-data-protection/*

key points relating specifically to ICT can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

For further information please see the GDPR Policy

Data Breach

In the case of a personal data breach, the data controller (TCES Group) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

For further information please see the GDPR Policy

7. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into School are entirely at the staff member, pupils & parents' or visitors' own risk. School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into School.
- Pupil mobile phones which are brought into School must be handed in on arrival at school for safe keeping.
- Staff (with the exception of DSL) should ensure their mobile phones are either in a locker or in the staff room during lesson periods. Staff members may use their phones during School break times but should be not be on their person during lessons.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided at all times
- The School reserves the right to search the content of any mobile or handheld devices on the School premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or pupils need to contact each other during the School day, they should do so only through the School's school telephone. If a staff member is expecting a personal call, they may leave their phone with the School office to answer on their behalf
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal School time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to School are the responsibility of the device owner. School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the School site, e.g. changing rooms and toilets.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices. In cases where an activity is taking place the school camera should be used, but not. without the prior consent of the person or people concerned.

Pupils' use of personal devices

- School strongly advises that pupil mobile phones should not be brought into School.
- School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches this policy, then the phone or device will be confiscated and will be held in a secure place in the School office. Mobile phones and devices will be released to parents or carers in accordance with this policy.

- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupils withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a School phone. Parents are advised not to contact their child via their mobile phone during the School day, but to contact the School office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Pupils will be provided with School mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a School phone where contact with pupils, parents/ carers is required.
- Mobile Phones and personally-owned devices will not be used during teaching periods. unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches this policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for School duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a School mobile phone will be provided and used. In an emergency where a staff member doesn't have access to an School-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In School:

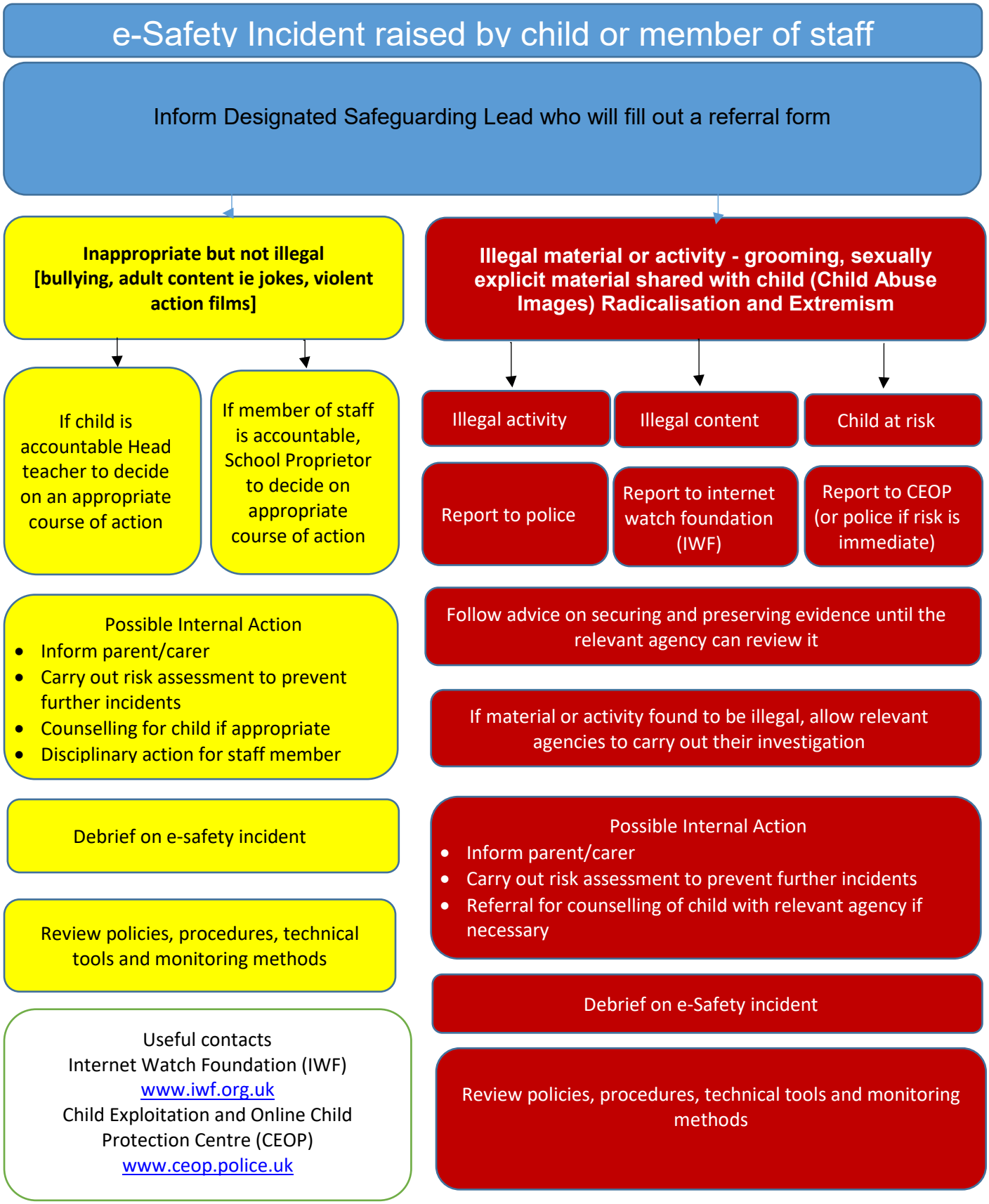
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the School agreement form when their child joins the School;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published School produced video materials / DVDs;
- Staff sign the Acceptable Use part of this Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the School web site, in the prospectus or in other high-profile publications the School will obtain individual parental or pupil permission for its long term use
- The School blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include Management Development Group, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or School. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all School-owned hardware will be recorded in a hardware inventory and kept locally at Central Services.
- Details of all School-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

8 Reporting Flowchart



8 Responding to E-Safety Incidents – Additional Notes

E-Safety Incident	An e-safety incident is one where the misuse of technology has had a negative impact on the safety, security or wellbeing of children or staff members
Capture evidence of activity or materials	This can be completed on a computer by taking a 'screenshot'. Press the 'Print Screen' button on the computer where the offending material is visible on the monitor. Open a second page and 'Paste' the image. Type under the image the computer number, the username and the name of the person taking the screenshot before saving this file
Illegal activity or materials found or suspected	Laws that may be contravened include: The Computer Misuse Act 1990, The protection from Harassment Act 1997, the Malicious Communications Act 1998, Section 127 of the Communications Act 2003
Consult with	Staff Consult with – Designated Safeguarding Lead (DSL) DSLs Consult with Police, CEOP or IWF
Report to Police	Contact your local Police station
Report to IWF	Internet Watch Foundation: www.iwf.org.uk
Report to CEOP	Child Exploitation and Online Protection: www.ceop.police.uk
Capture, Secure and preserve evience of activity or materials	Use the screenshot method listed above but in the presence of a witness to demonstrate you have not tampered with the evidence. Sign a print out the evidence file and have the witness countersign it. Then remove the computers involved from the network and store them securely. If the evidence is on a mobile device, then confiscate the devise.
Remove offending materials and/or content where possible	The pupil who published the offending information is most able to remove it. If you are unable to encourage this course of action, pages 5&6 of the DfE: Advice for Head Teachers and School Staff, outlines a range of strategies that can be used for different online services including Facebook, Youtube etc. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Key Contacts & Designated Safeguarding Leads (DSLs)

East London Independent School (ELIS)

- Adel Stedman Head Teacher 020 8555 6737
  adel.stedman@tces.org.uk
- Ishamar Blake, Deputy Head, 020 8555 6737
  Ishamar.blake@tces.org.uk
- Alicia Pennant, Assistant Head 020 8555 6737
  Alicia.pennant@tces.org.uk

North London Independent School (NWL)

- Katrina Medley, Head Teacher 020 8749 5403
  Katrina.Medley@tces.org.uk
- Dale Brown, Deputy Head, 020 8749 5403
  Dale.Brown@tces.org.uk
- Corinne Hyman, Inclusion Manager 020 8749 5403
  Corinne.Hyman@tces.org.uk

Essex Fresh Start Independent School (EFS)

- Cheryl Rutter, Head Teacher 01376 653 170
  Cheryl.Rutter@tces.org.uk
- Sue O'Sullivan, AHT & Site Lead, Witham 01376 653 170
  Susan.O'Sullivan@tces.org.uk
- Elainor Lloyd, AHT & Site Lead, Clacton 01255 225 204
  Elainor.Lloyd@tces.org.uk

Create London (part of both London Schools)

- Evangelia Theochari Co Head 020 8543 7878 Evangelia.Theochari@TCES.org.uk
- Amanda Cox, Education Case Coordinator, 020 8591 8692
  Amanda.Cox@tces.org.uk
- Mark Farlow, Inclusion Manager, Custom House 01708 393 150
  Mark.Farlow@tces.org.uk

Central Services Coordinator:

- Thomas Keaney, School Proprietor, 0208 543 7878 thomas.keaney@tces.org.uk
- Sonia Ghaznavi, Child Protection and Safeguarding Lead, 020 8543 7878 Sonia.Ghaznavi@tces.org.uk

Appendix 1 : Acceptable Use Policy – Staff Agreement Form

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in School: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the School's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head teacher.
- 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 email / Internet / intranet / network.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the School's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any School business.
- I will only use the approved School email, School Learning Platform or other School approved communication systems with pupils or parents/carers, and only communicate with them on appropriate School business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / School named contact.
- 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 to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the School's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use a USB under any circumstances to save or transfer data. *(the only acceptation to this is the downloading of CCTV footage for specific reasons which include 'evidence for police when a criminal activity has taken place or when a DSL needs to retain CCTV for an ongoing investigation)*
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff or store images at home
- I will use the School's Learning Platform in accordance with School protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop loaned to me by School, is provided solely to support my professional responsibilities and that I will notify the School of any “significant personal use” as defined by HM Revenue & Customs.
- I will access School resources remotely (such as from home) only through the School /TCES approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow School data security protocols when using any such data at any location.
- I understand that GDPR requires that any information seen by me with regard to staff or pupil information, held within the School’s information management system, 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.
- I will embed the School’s e-safety curriculum into my teaching.
- I will alert the School’s named DSL if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-School safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the School.

I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): 'Staff' agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand School's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the School ICT resources and systems.

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

Full Name ..... (printed)

Job title .....

Company Name: ……

Authorised Signature

I approve this user to be set-up.

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

Full Name ..... (printed)

Appendix 2: Children and Young Adult Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

TCES Group believes that Children and Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that children and young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Pupil Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when online.
- 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 to my school or parent/carer any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

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

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

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

- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

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

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

- I understand that I am responsible for my actions, both in and out of school

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions. This may include loss of access to the school network / internet.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student/Pupil Acceptable Use Agreement Form
This form relates to the student / pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to
the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

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

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, BYOD
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school,
- Accessing school website etc.

Name of Pupil _____

Name of School & Site _____

Class Year _ _____

Signed _____ Date_____

Appendix 3: e-Safety Agreement Form – Parents

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the School to give my *daughter / son* access to:

- the Internet at School
- School's chosen email system
- School's online managed learning environment
- ICT facilities and equipment at School.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the School takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the School can, if necessary, check my child's computer files and the Internet sites they visit at School and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the School has a clear policy on "The use of digital images and video" and I support this.

I understand that the School will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the School may use photographs / video that includes my child in publicity that reasonably promotes the work of the School, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at School events without permission.

Social networking and media sites: I understand that the School has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the School takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the School by promoting safe use of the Internet and digital technology at home. I will inform the School if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with GDPR, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at School include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
- e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian. Your child's image being used for presentation purposes around School; e.g. in class or wider School wall displays or PowerPoint presentations.
- Your child's image being used in a presentation about the School and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, Schools or educators;
- e.g. within a CDROM / DVD or a document sharing good practice; in our School prospectus or on our School website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

School asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- *We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.*

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the School and can potentially lower School's (or someone in the School) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.
The whole School community is reminded of the CEOP report abuse process: https://www.thinkuknow.co.uk/parents/browser-safety/

Appendix 4: TCES Group Parental ICT Charter

TCES Group Parental ICT Charter

As part of East London Independent School's Information and Communication Technology (ICT) programme we offer pupils supervised access to the Internet on the school premises. Access to the Internet will enable pupils to explore thousands of libraries, databases, and exchange messages with other Internet users throughout the world. While this has huge educational benefits, parents/carers should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. We hope however, that this should be minimal, as we currently us ***Impero Education Pro website filtering software*** which is monitored by our external ICT company called Onsem who filter the material, though no guarantees can be given.

During school, teachers will guide pupils towards appropriate materials within our dedicated ICT Suite. Outside school, particularly whilst using the school learning platform, parents/carers bear the same responsibility for such guidance as they exercise with television, cinema, and videos.

Pupil guidelines
Pupils are responsible for good behaviour on the Network, Internet and Learning Platform just as they are in a classroom or a school corridor – general school rules apply. Remember, the Network, Internet and Learning Platform is provided for pupils to conduct research and communicate with others for schoolwork. Access is a privilege, not a right and that access requires responsibility. Users should not expect that files stored on servers in school will be private; staff reserve the right to log and view files to ensure that users are using the system responsibly.

The following are not permitted
1. Sending or displaying offensive messages or pictures
2. Using obscene language
3. Harassing, insulting, misleading or attacking others
4. Damaging computers, computer systems or computer networks
5. Violating copyright laws
6. Using others' passwords
7. Trespassing in others' folders, work or files
8. Intentionally wasting limited resources by excessive or unnecessary printing
9. Accessing inappropriate services such as chat rooms, messaging services, auctions, live radio, music/video downloads, except when asked to do so as part of your work.

(in fact some of these are a criminal offence)

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet, network or learning platform use

2. Additional disciplinary action may be added in line with existing school policy on inappropriate language or behaviour

3. When applicable, local authorities or police may be involved.

Pupil name ……

I agree to comply with the school rules on Internet and computer network use.

Student signature ……

I give my permission for my child(ren) to the internet. I understand that pupils will be held accountable for their actions. I accept responsibility for setting standards for them to follow when exploring information and media.

Parent/Carer signature ……

Date…….