Last updated: August 2021 (AP)
Review date: August 2022

E-Safety Policy

(Written to comply with DfE statutory guidance – Keeping children safe in education, September 2021)

Introduction

Technology plays an important role at TLG and over the Covid-19 pandemic has proved to be more important than ever. It is often used within lessons as a central resource to help with the educational development of our students. Furthermore, it helps with the administrative side of our work with young people and is key to all online learning taking place across our Education Centres.

However, whilst the educational possibilities of using ICT are rapidly developing, all users of technology need to be alert and responsive to the potential dangers and risks associated with its use. These include:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

At TLG, we understand the responsibility to educate our students on e-safety issues; teaching them appropriate behaviour and skills to enable them to remain both safe and legal whilst using technology for learning or socially.

This policy aims to highlight some of the issues associated with ICT and provides guidance on how ICT should/could be used.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head Teacher and Management Committee have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the TLG Centre community need to be aware of the key people responsible for e-safety. At least one member of the TLG Education Centre Development (ECD) Team (which provides senior strategic leadership to all TLG Centres) needs to have undertaken training by a recognised organisation to deal with issues relating to e-safety and to allow training to be given to staff.

There is an expectation that Head Teachers/Deputies and Management Committees regularly access this policy on an annual basis. It is their duty to ensure they have an understanding of the issues and strategies at their Centre in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Management Committee members, visitors and students, is to protect the interests and safety of the whole TLG Centre community. It is linked to the following mandatory school policies on safeguarding and child protection, health and safety, student conduct agreement, and behaviour (including the anti-bullying) policy and PSHE.

Social Networks

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

Facebook, Twitter, Snapchat, Instagram, You Tube, online gaming and other forms of social media are increasingly becoming an important part of our daily lives. However, our students often misuse social networks, including by sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. In addition, there is an increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet.
Therefore, the use of social networks at the TLG Centre is not allowed and students take part in lessons highlighting the risks when using the internet and social networks in their own time.

- Staff are not permitted to access their personal social media accounts using TLG equipment during working hours. If staff are using TLG equipment to access social media outside of work hours, they must be mindful of the fact that data will be stored locally within the device history, that they need to log out at the end of the session and that login details should not be auto-filled or remembered by the device.
- Students are not permitted to access their social media accounts whilst at school on ANY device be it TLG equipment or that of their own.
- Staff, management committees, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, management committees, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, management committees, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.
- Staff should not befriend current students on social networking sites and best practise is to wait until that pupil is 19 before doing so (if necessary).
- Staff are not permitted to post any information or images regarding students or their centre on social media using their private account. Any posts for TLG should be made on the relevant TLG pages by the TLG Communication Team, this can then be shared by others when available.
- It is recommended that all staff, who have private social media accounts change their user names to one where their identify can't be easily identified and privacy setting should be set to the maximum protection.

Mobile and Smart Technology

Students may bring mobile telephones or smart devices to the TLG Centre but they must be on silent or switched off and handed in to staff at the beginning of the school day. Students may be permitted to have their phones or devices back for a specified period within the lunch-break to check for messages, provided they are then handed back to staff until the end of the day. Students are not permitted to access social networks on their devices during this time and staff should provide an adequate level of supervision to ensure this does not happen. The privilege of having access to their phone or device during lunchtime will be withdrawn for any student that does not comply with this expectation. There should be no need for students to make or receive calls from their mobiles in the Centre – all phone calls should be made or received on the TLG Centre Phone.

Use of the Internet – including Filtering

Staff and students are able to access a wealth of information via the Internet to help with education/study. It is important though that the Internet is not used excessively and is well planned into the curriculum. The TLG Centre provides students with supervised access to Internet resources through the use of Barracuda software. Websites and their content are filtered by Barracuda and Centres can add to the list of blocked sites flexibly and quickly. TLG's IT support provider (currently Pure Tech) centrally control this.

Staff should preview any recommended sites before use to check that they work on the school system and are appropriate, including checking that they do not contain any terrorist or extremist material.

Raw image searches are discouraged when working with students and key search terms are provided to students.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute TLG-owned software or illegal software from other sources

All users must observe copyright of materials from electronic resources.

The Internet should be used primarily for educational purposes. Where students are given permission to use the Internet recreationally, close supervision must be given to the sites they are visiting and content they are viewing.

Should you come across a website that is inappropriate it is important to alert Pure Tech to these to allow the website to be blocked across the organisation and in the short-term, to block it locally using Pure Tech. If you wish to access a website that is blocked centrally, you may request for this to be unblocked, again by contacting Pure Tech. This website will be checked and a request sent through to a senior leader of the school to confirm acceptance of this.

There should be no attempt to access sites deemed inappropriate as this may trigger an alert on the monitoring system. If any pupil uses the Internet inappropriately, this should be logged with the Head Teacher and the E-safety Lead should be made aware of all significant or ongoing concerns.

Monitoring

Authorised ICT support staff may access ICT equipment that is owned / leased by the school at any time with prior notice. Generally, this will be completed by a representative from TLG's ICT support service provider for the school, currently Pure Tech.

In certain circumstances the Head Teacher or a senior member of TLG staff may instruct the service provider to monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other form of electronic communication involving any student or employee, without consent, to the extent permitted by law.

Occasions where this may be necessary include

- Confirming or obtaining school business related information
- Confirm or investigate compliance of school standards, policy and procedures
- Quality control or training purposes
- Prevent or detect crime
- Child protection

All monitoring, investigative and surveillance work should be conducted by authorised ICT staff and comply with the Data Protection Act 1998, Human Rights Act 1998, Regulation of investigatory Powers Act 2000 and the Lawful Business Practises Regulations 2000.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

All Internet activity is filtered by TLG's internet provider. Browsing history may be monitored by the Centre if there are suspicions of misuse. The TLG Centre uses Barracuda software to filter internet use and to view and control student computer use.

Online Distance Learning - Staff

At TLG we offer weekly online virtual learning lessons to some students who attend five days a week. We also use online/ distance learning/check ins for students who may be isolating due to Covid 19 or centres that are having to temporarily close due to Covid 19 circumstances. TLG's basic rule for on-line virtual lessons and check-in's is: 'if you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.'

- You must only use TLG registered accounts for Teams/Zoom/ Google Classroom or any other platform, never personal ones.
- If using Zoom meeting software, you must ensure that the link or meeting ID and password to the meeting is sent to parents/ carers and not direct to students. If for whatever reason this isn't possible then notify parents/ carers that an invitation is coming from you to their child before you send it and then check with them that it has arrived.
- Students, staff and parents should be reminded about the AUP agreements they signed before online distance learning takes place.
- Students and staff should be reminded about the safeguarding policy and reporting process before any online learning take place.
- You must always check your settings as the host (who can chat? who can start a stream? who can join? Who can share screen?) and remember to end the meeting at the end of the session.
- As the host of a Teams/Zoom conference call always use the lobby/waiting room facility to check who is accessing the meeting and make sure students log in with their name.
- Don't turn on streaming for students by mistake – joining a stream does not equal starting a stream.
- As in the classroom make sure that the students are aware of the ground rules for the online lessons. When can they speak / how? How can students ask questions or get help?
- Cameras for staff and students should be turned off, unless it is a student check in or online student induction (where the student is in centre) and more than 1 member of staff is available.
- Avoid 1:1 sessions. Where possible always aim to have a group of students involved. If this isn't possible due to it being a student check-in then ensure that another member of staff is involved in the session.
- The live class/ session should be recorded so that if any issues were to arise, the video can be reviewed. Parents/ carers and students should be made aware of this procedure before you set up any sessions and you should have their verbal permission to do this.
- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible somewhere parents/ carers can check in on.
- Live classes should be kept to a reasonable length of time
- Language must always be professional and appropriate
- Staff must only use platforms that they have approved with the ECD team to communicate with students
- Staff should record attendance to online learning lessons using the register on Lighthouse.
- Staff should record the length, time, date and attendance of any student check ins.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

Online Distance Learning - Students

Distance learning requires teachers and students to adapt normal classroom routines to the online world, but the normal high expectations of respectful behaviour will remain. These expectations are consistent with TLG's e-safety policy and the previously signed ICT acceptable use agreement.

- The recording of still images, filmed images or audio of staff or other pupils without permission, and the distribution of such images, is strictly forbidden.
- Any meeting recordings that are uploaded to Teams are for use in the lesson only and must be kept on Teams and not attempted to be downloaded.
- Making inappropriate, offensive or unkind comments, including through emojis and/or images, will not be tolerated. Any profile names used for on-line and distance learning must follow teacher recommendations.
- Any visual or audio file shared with others must be appropriate to the learning task. Staff will check the suitability of any files uploaded by students and will follow normal discipline procedures if inappropriate material is discovered.
- There is an expectation that students will engage in online collaborative work when requested by their teacher, work in a respectful and helpful manner, following instructions carefully.
- Students are expected to take reasonable steps to complete learning tasks in the timescales set by teachers so as to maintain progress in their studies. Distance learning requires greater self-management of task completion by students, given the absence of physical face-to-face teacher contact. Staff will be understanding in regards to genuine reasons for delays to the completion of set tasks so it is important to keep in regular contact to inform them of any issues that might cause delays in the completion of set work.
- It is expected that students will engage in any on-line lessons in a manner as similar to regular classroom learning as possible. This includes: not lying in bed; making sure no music is on in the room; mobile phones are not to be used during the lesson unless directed by the teacher, nor are other functions on computers or games.
- Students are not permitted to share links/ meeting I.D./ log-ins or passwords to online conference sessions with anyone else outside of the invited group.

  NB – for students who take part in Online Learning there is only an online student conduct agreement.

Acceptable Use Agreements

Each year, ALL staff employed at the Centre shall undertake some training with regards to e-safety. As part of this training, all employees should sign an Acceptable Use agreement and this must be held by the Head Teacher.

All students should take part in one dedicated lesson at the start of the year (or when they start at the centre) where e-safety is addressed and students re-sign an Acceptable Use Agreement.

A copy of the staff, pupil and parent agreements can be found in the appendices of this policy.

Parents should be alerted to the e-safety policy during the referral interview, through the *referral form* and it should be made available as a hard copy or electronically if requested. The e-safety policy and additional information related to e-safety is accessible from the TLG Centre website. Parents should sign the AUP and read the school e-safety policy during the referral interview before their child starts at TLG. They should also be aware of and give consent to any guidance for online distance learning. E.g. All meeting will be recorded.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

E-Safety in the ICT and PSHCE Curriculum

E-safety is securely embedded into the ICT curriculum. It is essential for students to receive the same message across faculty areas and to learn the skills necessary for staying safe using ICT. Below are some areas covered in the ICT Curriculum.

- Staying Safe online in each of the 4 areas of risk (content, contact, conduct and commerce) and also recognising and guarding against radicalisation
- Social Networks
- Cyberbullying
- Sexual harassment
- Sexting or youth produced sexual imagery
- Copyright and keeping information safe and secure
- Legislation relating to computers and technology
- Respecting information
- Using correct appropriate search techniques

Cross Curricular E-Safety

ICT now plays a key part in the education of students. ICT is used widely for research and to enhance the quality of work produced by students. It is important that teaching and learning incorporates the use of ICT and that when planning and delivering lessons using ICT, matters relating to e-safety are considered by all staff.

Staff Training

Training will be provided annually to all staff as part of the introduction to the new school year. This will be focussed on keeping students safe and managing risk. Regular information on e-safety will be provided to staff to keep staff abreast of developments. Over the school year, there may be opportunities for staff to attend additional training events. Information about these will be published when available.
All staff will review the acceptable use agreement on an annual basis and sign the document to acknowledge their professional responsibilities in relation to ICT in general. New staff starting midyear will need to sign this as part of their induction.

TLG Lighthouse Information Management System (Lighthouse)

Lighthouse allows staff to access the data that is stored in this information management system from anywhere. This Policy applies wherever access to Lighthouse is provided and whenever information is accessed through Lighthouse. This policy applies whether or not the computer equipment used is owned by TLG. The policy applies to all those who make use of TLG's Lighthouse system.

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of TLG's data, the authorised Lighthouse user and the individuals to which the Lighthouse data pertains. In particular, these risks arise from:

- The intentional or unintentional disclosure of login credentials to Lighthouse by authorised users

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

- The wrongful disclosure of private, sensitive and confidential information
- Exposure of TLG to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the GDPR 2018 are adhered to. This Policy aims to promote best use of the Lighthouse system to further the communication and freedom of information between TLG and Parents/Carers.

Lighthouse Usage Policy Rules

Lighthouse Users

Lighthouse is provided for use only by persons who are currently employed by TLG or the TLG Centre, for students, or those who have legal responsibility for students attending the Centre. Access to the functions of Lighthouse and information contained within it is tailored dependent on the roles and responsibilities of the user.

Personal Use

Information made available through Lighthouse is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from Lighthouse to any person(s) with the exception of the students to which the information relates or to other adults with parental responsibility.
- Users should not attempt to access Lighthouse in any environment where the security of the information contained in Lighthouse may be placed at risk, e.g. a cybercafé.

Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password. You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

Passwords for any users other than students, will be issued by TLG HR and cannot be changed by the user. Passwords for students will be issued by Centre staff and can be changed by Centre staff.

TLG reserves the right to revoke or deny access to Lighthouse of any individual under the following circumstances:

- Users found to be in breach of this policy
- Users no longer employed by TLG or the TLG Centre.

If any child protection concerns are raised or disputes occur, TLG may revoke access for all parties concerned pending investigation.

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

TLG Email System – Staff

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

The use of email within TLG is an essential means of communication for staff. In the context of TLG and the TLG Centre, **e-mails CANNOT be considered as private and should therefore only be used for official TLG business.**

- TLG gives each member of staff an email account in order to protect staff and minimise the risk of receiving malicious / unsolicited emails.
- All email may be filtered and logged and email histories may be re-traced. Therefore, it should only be used for official TLG business
- Users should keep passwords and account details secure.
- Students / parents / carers should, under no circumstances, be contacted by staff using their personal email address.
- When sending an email from a TLG account, it should include the standard disclaimer statement – this provided by the TLG Communications Team. This is to protect TLG and ensures personal responsibility from the user.
- Emails should be carefully checked before sending as any content signifies official TLG correspondence, similar to that of letters being sent using letter headed paper.
- Emails created on a school account will be subject to disclosure should a request be made under the Freedom of Information Act 2000.
- Staff MUST inform their line manager / eSafety co-ordinator of any offensive emails they receive.
- Send emails to intended recipients only. Do not send blanket emails unnecessarily.
- Only send attachments to intended recipients.
- Check emails regularly and delete unwanted items.
- Never open attachments from unwanted / unknown sources.

Email for TLG Students

TLG provides a dedicated in-house email system for students using Outlook via Office 365. When students start in centre, they will be assigned a TLG email address through Outlook /Office 365 account for use in online learning and ICT lessons and the wider curriculum. Students may not use these until they have covered safe use of the Office 365 system in a dedicated ICT lesson. Students may also use email accounts provided by their referring schools should they need to.

- Student users are expected to adhere to general good practice guidelines of netiquette (delivered in ICT lessons). Language should be appropriate and they should not reveal any personal information about themselves to other people.
- Students should be aware that all email may be filtered and logged and email histories may be re-traced, therefore it should only be used for TLG learning and school work.
- TLG gives each student an email account in order to protect students and minimise the risk of receiving malicious / unsolicited emails.
- Students should keep passwords and account details secure.
- When sending an email from a TLG account, it should include the standard disclaimer statement – this provided by the TLG Communications Team. This is to protect TLG and ensures personal responsibility from the user.
- Emails should be carefully checked before sending as any content signifies official TLG correspondence, similar to that of letters being sent using letter headed paper.
- Emails created on a school account will be subject to disclosure should a request be made under the Freedom of Information Act 2000.
- Students MUST inform their Head Teacher / DSL of any offensive emails they receive.
- Check emails regularly and delete unwanted items.
- Never open attachments from unwanted / unknown sources.
- At KS3, students should use emails under general supervision and should form a structured part of the lesson.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

- At KS4, students may use email more freely but staff should still regulate its use in lessons.

Use of Digital Images and Video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the TLG Centre community or public, without first seeking consent and considering the appropriateness.

- Not all parents' give permission for photographs of students to be taken. This information can be found on Lighthouse and must be adhered to as there are often safeguarding reasons why photographs should not be taken and used.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. If the TLG centre has a mobile phone for staff use that belongs to the centre and remains in the centre then this may be used to photograph students. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Head Teacher.
- Where digital images / photographs are used and shared publicly, students' first names only should be used.
- For the protection of all involved online lessons will be recorded and they will be kept in line with our GDPR requirements.

Misuse of ICT

- Complaints of Internet Misuse must be reported and dealt with by the Head Teacher, Management Committee or TLG e-safety Lead.
- Any complaint about staff misuse should be directed to the Head Teacher, Management Committee or TLG e-safety Lead.
- Complaints of a child protection nature should be referred in the usual manner to the centre-based Designated Safeguarding Lead.

Reviewing Online Safety

TLG's E-Safety Lead will carry out an annual review of our approach to online safety, which will be supported by an annual risk assessment that considers and reflects the risks our students face. Issues arising from this will be incorporated into written policies and procedures and addressed during annual staff training.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

Relevant Legislation

Acts Relating to Monitoring of Staff email

- **General Data Protection Regulations 2018**
  The Regulations requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. It grants individuals rights of access to their personal data, compensation and prevention of processing.

  http://www.hmso.gov.uk/acts/acts1998/19980029.htm
  The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

  http://www.hmso.gov.uk/si/si2000/20002699.htm
  Regulation of Investigatory Powers Act 2000

  Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
  http://www.hmso.gov.uk/acts/acts2000/20000023.htm

- **Human Rights Act 1998**

  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to E-Safety

- **Racial and Religious Hatred Act 2006**
  It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

- **Sexual Offences Act 2003**
  The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
  For more information www.teachernet.gov.uk

- **Communications Act 2003 (section 127)**
  Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently

making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

- **The Computer Misuse Act 1990 (sections 1 – 3)**
  Regardless of an individual's motivation, the Act makes it a criminal offence to gain: access to computer files or software without permission (for example using another person's password to access files) unauthorized access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or program.
  UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

- **Malicious Communications Act 1988 (section 1)**
  This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

- **Copyright, Design and Patents Act 1988**
  Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

- **Public Order Act 1986 (sections 17 – 29)**
  This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

- **Protection of Children Act 1978 (Section 1)**
  It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

- **Obscene Publications Act 1959 and 1964**
  Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

- **Protection from Harassment Act 1997**
  A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
  A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

- **General Data Protection Regulations 2018**
  https://gdpr-info.eu/

- **The Freedom of Information Act 2000**
  http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

TLG - The Education Charity, National Support Centre, Hope Park, Bradford, BD5 8HH
Web: www.tlg.org.uk, email:info@tlg.org.uk, Tel: 01274 900373

Appendix A: TLG E-Safety – Staff Code of Conduct for ICT / AUP

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult TLG's e-safety policy for further information and clarification.

- ☐ I understand that it is a criminal offence to use ICT system for a purpose not permitted by its owner.
- ☐ I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for TLG business.
- ☐ I understand that TLG information systems may not be used for private purposes without specific permission from the Head Teacher.
- ☐ I understand that my use of TLG information systems, internet and email may be monitored and recorded to ensure policy compliance.
- ☐ I will respect security and I will not disclose any password or security information to anyone other than an authorised system manager.
- ☐ I will not install any software or hardware without permission.
- ☐ I will ensure that personal data is stored securely and is used appropriately, whether in TLG, taken off the TLG premises or accessed remotely.
- ☐ I will respect copyright and intellectual property rights.
- ☐ I will follow all online/distance learning /check in procedures as outlined in the e-safety policy
- ☐ I will report any incidents of concern regarding children's safety to the e-Safety Lead, and the centre-based Designated Safeguarding Lead.
- ☐ I will ensure that electronic communications with students including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- ☐ I will ensure that my use of ICT systems privately (e.g social networking, text messaging) will not crossover with my ICT use professionally by protecting my social networking profiles from public view, and not giving out personal contact information **I will not add current students as friends on social networking sites, and will take care to ensure that any comments about TLG/TLG activities are appropriate and professional.**
- ☐ I will not post any information or images regarding students or my TLG Education Centre on social media using my private account.

TLG may exercise its rights to monitor the use of the TLG's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the TLG's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:..... Print name:……..... Date: .....

KS3/4 Student Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's IT equipment for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not access any of my social media accounts on any device while at TLG, including devices owned by TLG and those that belong to me.
3. I will not bring files into school that can harm the school network or be used to circumvent school security tools.
4. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
5. I will keep my logins, IDs and passwords secret and change my password regularly.
6. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
7. I will only e-mail or contact people I know, or those approved as part of learning activities.
8. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
9. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
10. If I take part in any online/distant learning or check ins, I will follow all online/distance learning /check in procedures as outlined in the e-safety policy.
11. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
12. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.
13. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
14. I am aware that some websites, games and social networks have age restrictions and I should respect this.
15. I am aware that my online activity at all times should not upset or hurt other people. This includes not taking or sharing any images, including of staff or other students which could be used to offend or deliberately hurt or upset them. I'm aware that procedures are in place to protect staff and students from this activity and that action will be taken against anyone who disregards this agreement.

I have read, understood and accept the Acceptable Use Agreement for ICT.

Signed:..... Print name:…….....Date: .....

Acceptable Use Policy (AUP) for PARENTS

What is an AUP?

We ask all students, staff and adults involved in the life of TLG to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP during their induction which will have been sent home to you.

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell students about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read TLG's full E-Safety Policy on the school's website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to the head teacher.

What am I agreeing to?

- I understand that TLG uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the young people in our care for their future lives.
- I understand that the school takes every reasonable precaution to keep students safe and to prevent them from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
- I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
- I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and

refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers.

- The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from students when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
- I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video/audio of my child for internal purposes such as recording attainment or during an online distant learning lesson The full details of how we use digital images and video are outlined on the following page where we ask you to give your consent.
- I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety. Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
- I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
- I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
- I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

The Use of Digital Images and Video

To comply with the Data Protection Act 1998, 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 student is named, we avoid using their photograph.

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

Where showcasing examples of students 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 students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film. Only images of students in suitable dress are used.
~~~~~~~~~~~~~~~~~~~~

Staff are not allowed to take photographs or videos on their personal equipment. Some staff do have school mobile phones that they may use to capture photographs as evidence for assessed work, these are not their personal phones and remain in school.

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

- Your child being photographed (by the class teacher or other member of staff) as part of a learning activity; e.g. taking photos or a video of art work or posters produced as evidence for a qualification.
- Your child's image being used for presentation purposes around the 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 DVD or a document sharing good practice; in our school prospectus or on our school website.
- Your child taking part in an online distant learning class/ session will be recorded so that if any issues were to arise, the video/audio can be reviewed, these recordings will be kept in line with our GDPR requirements and won't be shared outside of TLG unless a safeguarding concern arises during the session.

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.

I give permission for my child to be photographed/ filmed as per the outlined arrangements.

Name of student_____ Date_____

Name of parent/ guardian_____ Signature_____