our policy on online safety

This policy should be read alongside our other policies, particularly our overarching safeguarding policy. This policy applies to all staff (paid staff), interns, volunteers and anyone working on our behalf.

our values

At Tubers we recognise that being online is an intrinsic part of life for young people. Being online can and should be a fantastic and safe experience for children, young people and adults. Like the physical environment, the online environment has risks. At Tubers we understand that if we're teaching young people to be fantastic online digital creators, we also have a responsibility to give them the knowledge and skills to be able to use that environment safely; to be positive and supportive online citizens; to be resilient; and to have the confidence to report any online issues that make them feel uncomfortable or unsafe.

why we have this policy

This policy exists to:

- Protect children and young people who receive our services and who make use of information/digital technology (such as the internet) as part of their involvement with us.
- Provide staff and volunteers with the principles that guide our approach to online safety.
- Ensure that as an organisation we operate in line with our values and within the law in terms of how we use information technology and behave online.

We recognise that:

- The welfare of the children/young people who come into contact with our services is paramount and should govern our approach to the use and management of electronic/digital communications technologies and online behaviour.
- All children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- The use of information technology is an essential part of all our lives; it's involved in how we as an organisation gather and store information, as well as how we communicate with each other. It's also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all. However, it can present challenges in terms of how we use it responsibly and, if misused either by an adult or young person, can be actually or potentially harmful to them or others.

We will seek to keep children and young people safe by:

- Having an online safety lead within our organisation.
- Developing a range of procedures that provide clear and specific directions to staff, interns, volunteers and the children and young people we work with on how to behave online and the appropriate use of information/digital technology.
- Supporting and encouraging young people using our service to use the opportunities offered by mobile/internet/digital technology in a way that keeps themselves safe and shows respect for others.

- Supporting and encouraging parents and carers to do what they can to keep their children safer online, and to behave as positive online citizens/role models for their children.
- Incorporating statements about safe and appropriate information/digital technology use and online behaviour in the codes of conduct for staff, interns, volunteers and children/young people.
- Developing an online safety agreement for use with young people and their parents/carers.
- Use our procedures to deal firmly, fairly and decisively with any examples of inappropriate information technology use and online behaviour, complaints or allegations, whether by an adult of a child/young person (these may include breaches of filtering, illegal use, downloading or creating indecent images of children, bullying or use of information technology to groom a child or to perpetrate abuse).
- Informing parents and carers of incidents of concern as appropriate.
- Reviewing and updating the security of our information systems regularly (and inviting independent organisations into our premises to review our practices).
- Providing adequate physical security for our information technology equipment.
- Ensuring that user names, logins, and passwords are used effectively.
- Using only official online accounts provided via the organisation and monitoring these as necessary.
- Ensuring that the personal information of staff, volunteers, interns and service users are not published on our website.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained and only for the purpose for which consent has been given.
- Risk assessing in advance any social media tools used in the course of our work with children, young people and families.
- Providing effective management for staff and volunteers on information/digital technology issues and online behaviour.
- Examining and risk assessing any emerging new technologies before they are used within the organisation.

We will remain vigilant and alert to online risks to children including (but not limited to):

- Grooming and the risk of online exploitation
- 'Sexting'(the sharing of indecent images)
- Bullying
- The threat of online radicalisation
- Inappropriate content
- Illegal content

In terms of the overall safety of the children and young people we work with, we will be alert to indicators of other abuse including:

- Physical abuse
- Emotional abuse
- Sexual abuse
- Neglect

Roles and responsibilities

Designated Safeguarding Lead

This person will be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact
- Potential or actual incidents of grooming
- Bullying

Our staff

Our staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and our online safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement.
- They report any suspected misuse or problem to the management team and Designated Safeguarding Lead for investigation/action.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official systems (i.e. not via personal online accounts/apps).
- Online safety issues are embedded in all activities.
- Children and young people have an understanding of responsible research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc during sessions and implement current policies with regard to these devices.
- In activities where internet use is pre planned children and young people should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Understand who to contact and in what circumstances if they have any queries relating to an online issue (for example by contacting the Professionals Online Safety Helpline).
- Ac t as positive role models and behave in an appropriate manner online (professionally as well as personally).

Children and young people

Children and young people using our services:

- Are responsible for using our digital technology systems in accordance with the Acceptable Use Agreement.
- Understand that they are only permitted to publish online content created at Tubers via the designated Tubers accounts (which will be restricted to staff access only), and that staff will monitor these accounts for the purposes of their safety.
- Understand that content created at Tubers must be checked/authorised by a member of Tubers staff, prior to publishing online (and that publishing will take place by staff only).
- Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand our policies on the use of mobile devices (including film and photography).
- Will have an understanding of our 'No Hate' / bullying policy.
- Should understand the importance of adopting good online safety practice when using digital technologies and realise that their online behaviour outside of our organisation, could impact on their membership with us.
- Where appropriate we will invite external partners into our organisation to engage with children and young people about online safety (this could include Devon and Cornwall Police and other relevant organisations).
- Will have an understanding that whilst we will make every effort to resolve any issues that arise in consultation with them and their parents/carers, we also have a duty to inform the proper authorities if we have a child protection/criminal concern relating to any child or young person we work with.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate and safe way. We will take every opportunity to help parents and carers to understand these issues. Parents and carers will be encouraged to support us in promoting good online safety practice and conduct at all times.

Parents and carers will be provided with information relating to the 'age restrictions' of relevant websites/social media platforms. Tubers does not endorse any child or young person registering for any website/social media platform if they are not of an appropriate age to do so. If parents/carers wish for their child/young person to be a member of Tubers, and for that child/young person to be able to publish content outside of Tubers, it is recommended that a family/parent account be used to do so to enable parents/carers to control what is published and to monitor accounts for safety.

Use of digital and video images

- Using digital and video images is the basis of what we do, and we will teach children and young people how to become online content creators. However staff, parents/carers and the children and young people we work with need to be aware of the risks associated with publishing digital images (and other content) on the internet. Whatever we publish online can remain there indefinitely, and could cause harm or embarrassment to individuals. We will educate those we work with about these risks and work to ensure that they leave a legacy of positive online content.
- All content created at Tubers will be published via Tubers accounts. Whilst Tubers will provide children and young people with the knowledge and skills to create and publish digital content, Tubers will not accept responsibility for any content posted by a young person using Tubers services, via alternative (i.e personal) accounts.
- When using digital images/content staff will inform and educate children and young people about the risks associated with the taking, use, sharing, publication and distribution of images/content. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).
- Written permission from parents or carers will be obtained before photographs/digital film of children/young people are published online at the start of each term. Given the nature of the sessions, unfortunately children/young people will not be able to take part in activities without this consent.
- Other than Tubers staff/volunteers taking images of children during their time with our organisation (for example taking part in an activity), for training or marketing/publicity purposes, no other individual may

take images/record film of any child or young person. Such images/film recorded at Tubers will only be published via designated Tubers online accounts (i.e. never using personal accounts/apps).
- Tubers staff will be responsible for authorising the publishing of all online content created by children and young people from the designated Tubers accounts.

Safeguarding data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Tubers will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- We have a Data Protection Policy.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Tubers Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices**.**

Communication

- All children and young people must immediately report to a member of staff, the receipt of any online/digital communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and must not respond to any such communication.

- Any digital communication between staff, interns, volunteers and children/young people, or parents/carers must be professional in tone and content at all times.
- Online/digital communication between staff, interns, volunteers and children/young people and parents/carers must only be via the organisations established communications accounts, and not under any circumstances via personal accounts. Should personal accounts be used for communication, staff will be subject to investigation, possible disciplinary action or child protection investigation.
- Children and young people should be taught about online safety issues such as the risks attached to the sharing of personal information. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Our technical infrastructure

At Tubers we are responsible for ensuring that our networks are as safe and secure as is reasonably possible.

- Our technical systems will be managed in ways that ensure that we meet recommended technical requirements .
- We will regularly review and audit the safety and security of our technical systems.
- Our servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to Tubers technical systems and devices.
- Content produced at Tubers will only be published by Tubers staff using designated Tubers accounts.
- Our internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Tubers staff will regularly monitor and record the activity of users to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Tubers systems and data.
- All Tubers systems will be protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the Tubers systems.

Social media – protecting professional identity

At Tubers we have a duty of care to provide a safe learning environment for everybody. Staff, interns and volunteers must demonstrate that they are positive online citizens and role models at all times.

Tubers provides the following measures to ensure reasonable steps are in place to minimise risk of harm to those using its services through:

- Ensuring that personal information is not published.
- Relevant training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance exists, including responsibilities, procedures and sanctions.
- Risk assessments are in place and reviewed regularly.

Tubers staff, interns and volunteers should ensure that:

- No reference should be made in personal social media use to children, young people, parents or carers in receipt of Tubers services.

- They do not engage in online discussion on personal matters relating to members of the Tubers community.
- Personal opinions should not be attributed to Tubers.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Whatever they publish online in a personal capacity must be appropriate as a professional working with children and young people.

When Tubers social media accounts are established there should be:

- A process for approval by staff.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts, including: Systems for reporting and dealing with abuse and misuse; and an understanding of how incidents may be dealt with under Tubers disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with Tubers or impacts on Tubers, it must be made clear that the member of staff, intern, volunteer is not communicating on behalf of Tubers, with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the Tubers are outside the scope of this policy

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Tubers.
- Tubers should effectively respond to social media comments made by others according to a defined policy or process (and such communication will only be responded to by designated Tubers staff).

Responding to incidents of misuse

At Tubers we may need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Tubers community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures

Responding to illegal incidents

Any suspected illegal incidents will be reported to Devon and Cornwall Police. In addition to contacting the local police, issues relating to specific incidents such as: extremist content online will be reported to www.gov.uk/report-terrorism; criminal content will be reported to the Internet Watch Foundation; grooming or other related behaviour will be reported to CEOP.

At Tubers we will make every effort to forge effective relationships with relevant partner organisations. We will engage with Devon and Cornwall Police and invite representatives (such as the local Police Neighbourhoods Team) to our premises to meet with staff, interns and volunteers on a regular basis.

Other incidents

It is hoped that all members of the Tubers community will be responsible users of digital technologies, who understand and follow our policies. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the staffing team will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Training

Tubers staff will be trained in online safety. Tubers staff cannot be considered to be 'online safety experts' but will take steps to ensure that their personal learning and development is sufficient to safeguard those who use Tubers services. Staff will also access relevant professional organisations when necessary such as the Professionals Online Safety Helpline. Other organisations will also be invited into Tubers to provide relevant training/learning for staff and children/young people.

Contact details

The person within our team responsible for Safeguarding (Designated Safeguarding Lead) is:
Nick Ellison
Email: team@tubers.uk

Telephone: 07837 340736

Policy review

This policy was created on 28 December 2016. We are committed to reviewing our policy annually. This policy will be reviewed on or before 28 December 2017.