Online Safety and Acceptable Use Policy

The Directors at The Teignbridge Community Project are responsible for ensuring that those benefiting from us or working with us are not harmed in any way. The Directors of The Teignbridge Community Project have a legal duty to act prudently, and this means that they must take all reasonable steps within their power to ensure that no one is harmed. It is particularly important where beneficiaries are vulnerable persons or children in the community.

This policy applies to all those involved in Turning Heads, including, but not exclusively, Directors, Management, Team Leaders, Employees, Contractors and Volunteers.

Scope of the Policy

This policy applies to all members of The Teignbridge Community Project community (including staff, clients, volunteers, parents/guardians/carers, visitors, community users) or anyone who has access to and are users of The Teignbridge Community Project digital technology systems.

The Teignbridge Community Project will deal with incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians/carers of incidents of inappropriate online safety behaviour that take place on The Teignbridge Community Project premises. Employees who are involved with incidents of online safety behaviour will also be dealt with inline with the Fair Disciplinary and Dismissal Policy. This also includes any incidents which bring the reputation of The Teignbridge Community Project into disrepute.

Role of the Board of Directors

Directors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the D*irectors* receiving regular information about online safety incidents and monitoring reports.

A member of the B*oard* has taken on the role of *Online Safety Director*. The role of the Online Safety *Director* will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs

All Teignbridge Community Project Staff
Are responsible for ensuring that:

- we have an up-to-date awareness of online safety matters.
- we have read, understood, and signed the staff acceptable use policy/agreement attached to this policy.
- we report any suspected misuse or problem to the On*line Safety Lead* for investigation/action/sanction.
- all digital communications with children/customers/clients/carers etc. should be on a professional level *and only carried out using official The Teignbridge Community Project' systems .*
- online safety issues are embedded in all aspects of the work we carry out and other activities in relation to this.
- we all understand and follow the Online Safety Policy and acceptable use policies.
- we all have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- we monitor the use of digital technologies, mobile devices, cameras, etc. in work and other work related activities, and implement current policies with regard to these devices.
- be aware of vulnerable adults/children who do not wish for their image or personal details to be shared on any social media platform.
- We do **not** engage with any conflicting social media engagement which could bring The Teignbridge Community Project into disrepute.

Designated Safeguarding Person

They should be trained in online safety issues and be aware of the potential for serious vulnerable adult/child protection/safeguarding 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
- online-bullying

Students/Clients:

- are responsible for using The Teignbridge Community Project's digital technology systems in accordance with the client acceptable user agreement
- have a good 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.

Parents/Guardians/Carers

Parents/guardians/carers play a crucial role in ensuring that their children/vulnerable adults in their care understand the need to use the internet/mobile devices in an appropriate way. The Teignbridge Community Project will take every opportunity to help parents/guardians/carers understand these issues through: *letters, website, social media and information about national/local online safety campaigns/literature.*

Parents, guardians and carers will be encouraged to support The Teignbridge Community Project in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images.

Community Users

Community Users who access The Teignbridge Community Project's programmes as part of the wider provision will be expected to sign a Community User, acceptable user agreement before being provided with access to The Teignbridge Community Project.

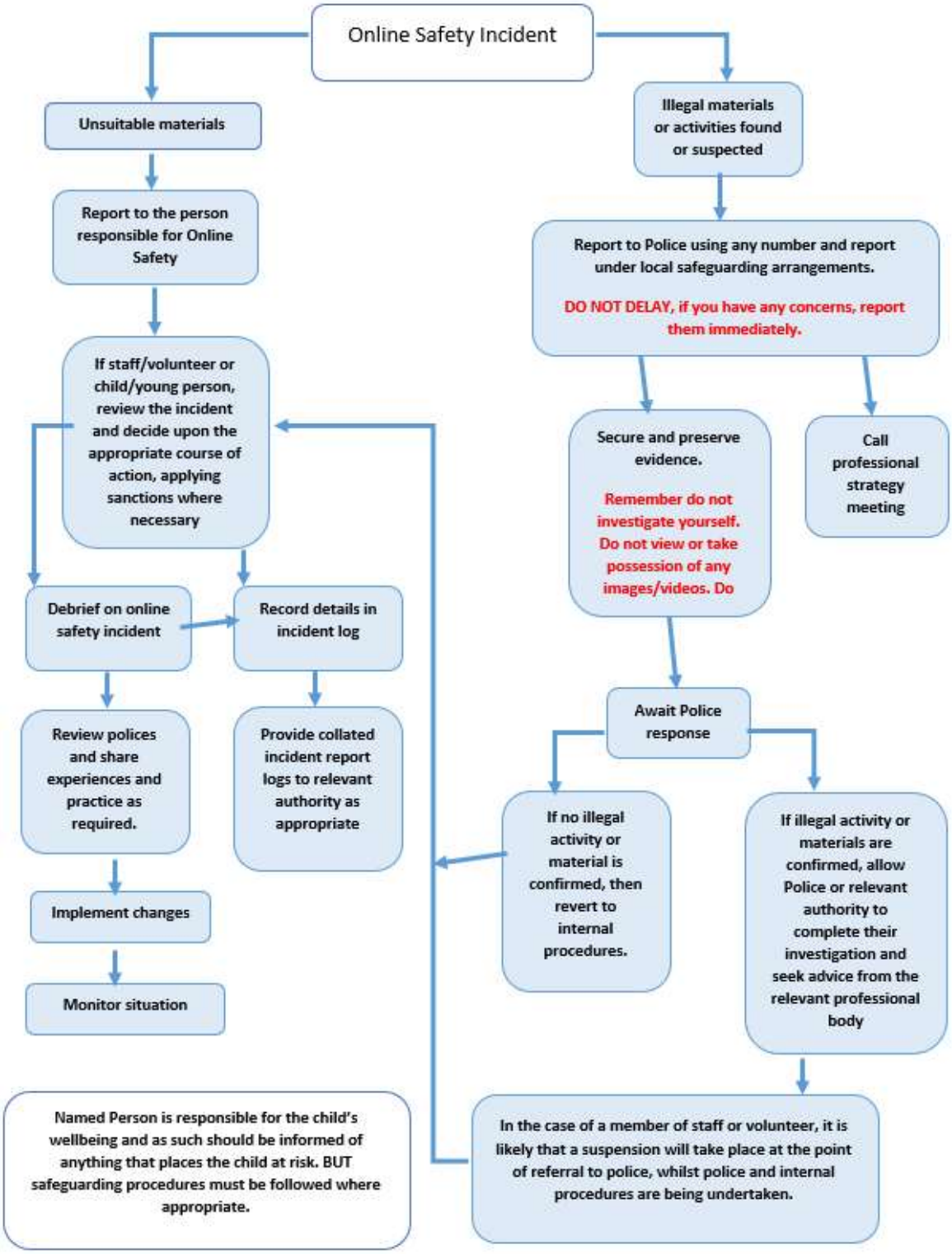
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

All members of The Teignbridge Community Project will be responsible users of digital technologies, who understand and follow policy. 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 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 group 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
    - Involvement by Local Authority/or national/local organisation (as relevant).
    - 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for The Teignbridge Community Project and possibly the police and demonstrate

that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Appointed Person

An appointed person should be made known to staff, volunteers and clients alike; as the designated person to whom concerns should be addressed.

The appointed person at The Teignbridge Community Project is:

Colette Palmer

Contact number: 07790930938

If the concern is about this designated person, please report to:

Anna Lofthouse

Contact number:07445158419

Reviewed: 1st August 2024

Next Review: 1st August 2026

Signed:

Date: 1st August 2024

Colette Palmer, Director

Signed:

Date: 1st August 2024

Anna Lofthouse, Director

Acceptable Use Policy

This agreement covers the use of digital technologies in The Teignbridge Community Project, including email, internet, shared network drives, network resources, all software, electronic equipment and all systems.

- I will only use The Teignbridge Community Project's digital technology resources and systems for professional purposes
- I will not reveal my password(s) to anyone
- I will follow 'best practice' advice in the creation and use of my password(s). If my password is compromised, I will ensure I change it
- I will not use anyone else's password, nor seek to discover it. If a colleague does reveal it to me, I will advise them to change it
- I will not allow unauthorised individuals to access any of The Teignbridge Community Project's systems
- I will ensure all documents and digital resources are saved, accessed and deleted in accordance with The Teignbridge Community Project's network and data security and confidentiality protocols
- I will not engage in any online activity that compromises my professional responsibilities, code of conduct or professional boundaries
- I will not browse, download or send material that could be considered offensive to colleagues or others
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to: Colette Palmer, Designated Safeguarding Lead or, Anna Lofthouse, Deputy Safeguarding Lead.
- I will not download any software or resources that can compromise the network, that breach a user's copyright, or are not correctly licenced
- I will not publish or distribute work that is protected by copyright
- I will not connect a computer, laptop, notebook or other electronic device (including USB flash drive) to the network that does not have up-to-date anti-virus software
- I will only use personal digital cameras or camera phones for taking and transferring images of children/young people/vulnerable adults or, staff/volunteers with permission, and will use those images only for their intended purpose

- I will ensure that any personal social networking sites/blogs, Twitter, Instagram accounts, etc., that I create or actively contribute to are separate from my professional role
    - It is my responsibility to ensure that my use of social networking sites/blogs, etc., does not compromise my professional role, and will ensure my privacy settings are appropriate
- Any computer, laptop or electronic device loaned to me by The Teignbridge Community Project is provided solely for professional use
- I will access The Teignbridge Community Project's resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those resources
- Any confidential data that I transport from one location to another will be protected by encryption
- I will follow The Teignbridge Community Project's data security protocols when using confidential data at any location
- Any information seen by me with regard to service users held within The Teignbridge Communtiy Project 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, e.g. Children's Social Care and/or the police
- It is my duty to support a whole organisation safeguarding approach and I will alert the The Teignbridge Community Project's named vulnerable adult/child protection officer/relevant senior member of staff if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern
- It is my responsibility to ensure that I remain up-to-date, read and understand The Teignbridge Community Project's most recent online safety policies
- I understand that all internet/network usage can be logged and this information can be made available to my line manager on request
- I understand that failure to comply with any aspect of this agreement could lead to disciplinary action
- I have read the Top Tips for internet security poster which is attached to this policy. I accept that this only covers the basics of Internet Safety.

I agree to abide by this Acceptable Use Policy at all times

I wish to have a network account; an email account; and be connected to all systems that are relevant to my post at The Teignbridge Community Project.

Full name ..... (printed)

Job title (If applicable) .....

Signature ..... Date: .....

Authorised signature

I approve this user to be set-up on The Teignbridge Community Project computer systems

Full name ..... (printed)

Job title .....

Signature ..... Date: .....

TOP TIPS

For Internet Safety

Stay anonymous!

- Use another name or a nickname
- Keep your address a secret
- Don't say where you go to school
- Only give your phone numbers to people you actually know
- Make sure you don't give ANY clues about yourself

Privacy!

- Always make sure your settings really ARE private so YOU choose who can see your account
- Don't give out any personal details
- Don't discuss your problems online
- If you think your account's been hacked, report it and change it

Think before you post

Don't post before thinking CAREFULLY and ask:

- Is it offensive?
- Could it affect your future employment?
- Would you be happy for your parents or family to see it?

WORK

Passwords

- Keep your password secure and change it regularly
- Don't use your name or anything easy to guess
- Don't share it with ANYONE, even your friends
- Use a mixture of capitals, numbers and special characters
- If in doubt CHANGE IT!

Remember...

- NOTHING is private
- Don't say anything you wouldn't say in real life
- Don't post other people's photos
- NEVER post invitations unless you are absolutely sure they will only be seen by a closed group

Are they real?

- Do you know this 'friend' in real life?
- Are you REALLY sure it's their account, not someone pretending to be them?
- Remember: some people are VERY clever at pretending to be someone they're not!

Feeling uncomfortable

- DON'T reply to trolls or people making unkind comments
- Don't be afraid to 'unfriend' or block people who upset you
- Do REPORT people if necessary

Believe ..... NOT!

- Don't fall for it - things aren't ALWAYS what they seem!
- Everyone exaggerates - you probably do it as well!
- Remember: most people only tell you the good bits!
- Don't be fooled by 'free' offers!

Be Safe! Be Sure! Be Smart!

www.loggerheadpublishing.co.uk