The Federation of Tiverton Schools

Heathcoat Primary School
Online Safety Policy

Status	**Statutory**
Person responsible for policy	**Demelza Higginson**
Policy to be implemented by:	**All members of the school community**
Version date:	**November 2023**
Review period	**2 years**
Date approved:	**22nd November 2023**
Signature of Co-Chair of Governors:	

Heathcoat Primary School
Online Safety Policy

Created: Autumn 2023
Next Review: Autumn 2025

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers, 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 Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. 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 Online Safety behaviour that take place out of school.

The internet provides both opportunities and threats to young people, such as bullying, grooming, exposure to pornographic materials, radicalisation & extremism and sexual exploitation. **Online safety is an umbrella term for promoting the safeguarding of children and young people when using any device over the internet.**

Definition of online abuse

Online abuse is abuse that is facilitated using technology. It may take place through social media, online games, or other channels of digital communication. Children can also be re-victimised if evidence of their abuse is recorded or uploaded online. Technology can facilitate a number of illegal abusive behaviours including, but not limited to: harassment, stalking, threatening behaviour, sharing indecent images of children under 18, inciting a child to sexual activity, sexual exploitation, grooming, sexual communication with a child and causing a child to view images or watch videos of a sexual act. Using technology to facilitate any of the above activities is online abuse.

Principles

- It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.
- However, we also need an understanding of the risks that exist online, so we can tailor our teaching and support to the specific needs of our pupils.
- We are committed to act on online safety incidents inside and out of school that affect pupil and/or staff wellbeing.

Teaching online safety

- We follow the DfE guidance “teaching online safety in schools” here
- Staff teach online safety through:
  - Our Computing curriculum (using Kapow)
  - Our PSHE/RSE curriculum (using Jigsaw)
  - Assemblies

    - Themed weeks e.g. Anti-bullying Week
- We use SAV (Stand Up Against Violence) trainers every other year to provide external support to pupils in Year 6 about staying safe online.
- Pupils in year 5 and 6 get an annual visit from a Police Officer on the theme of online safety.
- We celebrate and take part in Internet Safety Day each year.

Each half term we teach the children how to stay safe online and behave in a respectable way.
Pupils are taught about online safety, potential risks and harms. This includes being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

We teach pupils to consider the way that they access online content. We cover the following:

CONTENT – is this age appropriate? What do I do if it isn't?

CONTACT – who can I contact on here? Who can contact me? Are they safe? Am I being safe? Protect personal information.

CONDUCT – show the same respect online as you would do face to face.

COMMERCE - NEW - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Support for parents

- We keep the child protection and e-safety page on our website updated for parents to refer to when needed.
- We regularly send online safety advice out to parents, either through the newsletter, Facebook or separate emails.

Support for staff

- Online safety is part of the annual safeguarding training.
- We have in-house refreshers on online safety during the school year.
- The DSL and DDSLs receive weekly online safety updates from external professionals, which are then shared with staff in weekly Monday briefings.

Use of technology in school

- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school uses a filter, or proxy, to guard against unwanted content, through SWGfL.
- Filtering logs are regularly reviewed by the DSL and any breaches of the policy are acted upon.
- There are clear and effective routes for users to report inappropriate content.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Pupil misuse of technology is dealt with following the school Behaviour Policy.
- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted upon and outcomes recorded by the DSL. All users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with the safeguarding policy and practice.
- Staff and volunteer use of technology is governed by the acceptable use agreement.
- Pupils annually sign the acceptable use agreements.
- Visitor use of technology is governed by the Safeguarding and Visitor Policy.

- Data protection protocols are covered in a separate policy.
- Pupils in Year 5 and 6 are allowed to bring mobile phones to school and store them, switched off, in the classroom if they need to use them after school. They must hand them to the teacher at the start of the day. For this privilege, they need to have signed a mobile phone contract. Mobile phones found on pupils during the school day are confiscated and given to parents at the end of the day.

Appendix

What are the risks?

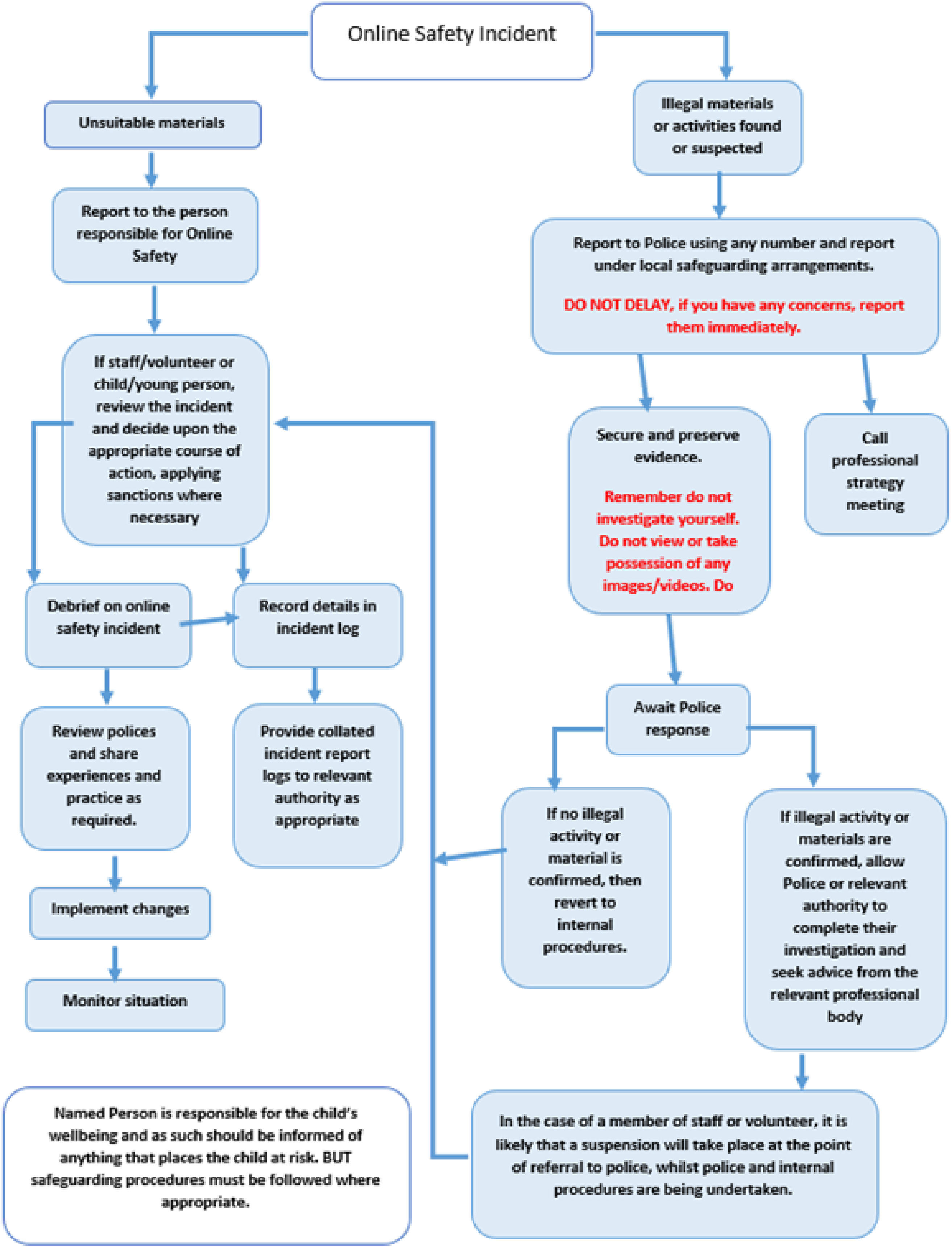
- grooming: through social media and/or gaming, this may involve radicalisation and/or sexual abuse;
- cyberbullying: can occur through any ICT, especially mobile phones;
- sexting: sending explicit or compromising photos or videos;
- sexual abuse: including non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways;
- financial: although this is rare towards children it does occur – online gambling is an increasing risk;
- exposure to inappropriate materials, racial hatred, frightening or pornographic pictures and videos;
- obsessive use of the internet and ICT, for example, addiction to video games;
- inappropriate or illegal behaviour, for example, exposure to hate mail or offensive images;
- copyright infringement, for example, the illegal sharing of music, pictures, videos or documents.

Spotting the signs

It is not always easy to spot signs of online abuse or lack of understanding of online safety. They may include:

- spending much more or much less time online, texting, gaming or using social media;
- appearing withdrawn, upset or outraged after using the internet or texting;
- being secretive about who they’re talking to and what they’re doing online or on their mobile phone;
- having lots of new phone numbers, texts or e-mail addresses on their mobile phone, laptop or tablet.

Dealing with an illegal incident:



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.