SHERWELL VALLEY PRIMARY SCHOOL

EXCELLENCE IN ALL WE DO

Sherwell Valley Primary School

Online Safety Policy

Approved by:	Headteacher	**Date:**	September 2023
Last reviewed on:	September 2023		
Next review due by:	September 2024		

This policy was written by the Online Safety team, building on best practice, government guidance and suggestions from the 360 Degree Safe Online Safety tool. It has been agreed by the Senior Leadership Team, Governors and Online Safety Champions.

This policy and its implementation will be reviewed annually. The next review will be September 2024 or more regularly in the light of any significant new developments in technology, new threats to online safety or incidents that have taken place in school. The demands of the 21st Century mean that our pupils will need to be alert to the new technologies and possibilities the internet can provide. We aim to ensure pupils are independently minded and confident citizens of the future.

Development / Monitoring / Review of this Policy

This online safety policy has been reviewed by a working group made up of:

- Headteacher & Designated Safeguarding Lead (Cristy Nelson)
- ICT Manager (Sharon Gilbert)
- Online Safety Curriculum Champions (Abby Mildoon & Sian Thompson)

Scope

This policy applies to all members of the school community (including staff, students/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 cyberbullying 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. 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. Staff behaviour online is also moderated via the school’s Code of Conduct.

Teaching and Learning

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- Sherwell Valley Primary School has a duty to provide pupils with quality internet access as part of their learning experience.
- Pupils use the internet widely outside school and need to learn how to keep themselves safe online.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions.

Benefits of using the Internet in education include:

- Access to worldwide online educational resources
- Learning and creating through apps
- Online learning platforms in school and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.

Online Safety Expectations

Education – pupils:
The education of Online Safety for pupils is an essential part of our school's Online Safety provision. The school will help and support the children to recognise and avoid Online Safety risks and to also build their resilience.

Online Safety education will be provided in the following ways:

- A planned Online Safety Curriculum is provided with explicit links made in the Computing and PSHE curriculum and is regularly revisited.
- Key Online Safety messages are reinforced to children in assemblies and in lessons.
- Pupils are taught in lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information.
- Pupils understand the need for the Pupil AUP (Acceptable Use Policy) and are encouraged to adopt safe and responsible use of Information and Communication Technology (ICT), the internet and mobile devices, both within and outside school.
- Pupils in Years 5 & 6 receive annual Online Safety training from an external provider, such as SWGfL.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers:
Parents and carers play an essential role in the education of their children and in the monitoring of their online experiences, therefore Sherwell Valley Primary School will communicate effectively with parents to bridge the digital divide. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, Newsletters, the School website, Tapestry and Class Dojo
- Online Safety evenings
- Parents' Evenings
- Reference to useful websites

Education & Training – Staff:
It is essential that all staff receive Online Safety training and understand this school policy and their responsibilities to it. Training will be offered as follows:

- Regular Online Safety Training and updates will be made available to staff.
- All new staff should receive Online Safety Training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Staff and Volunteer Acceptable Use Policies.
- All staff must read this Online Safety Policy.

How will information systems security be maintained?

Virus protection is currently provided by Sophos. Portable media e.g. external hard drives, memory sticks, SD cards etc. may not be used without specific permission followed by a virus check.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal camera devices including mobile phones				✓				✓
Use of hand-held devices eg iPods, PSPs, Nintendo DSs (provided by school)	✓					✓		
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails	✓							✓
Use of online storage facilities (e.g. Dropbox, G-Suite) to store non-sensitive data	✓							✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓*				✓
Use of blogs	✓					✓		
Use personal email to send school related communications				✓				✓

✓* Except at social times e.g. in the staff room on lunch break

For the case of residential trips, staff must use a school device to take photos of the children. These can then be uploaded to Dojo/Tapestry inorder to keep parents informed.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored. When staff leave the employment of SVPS, their account will be suspended and made available for checking in the event of any allegation arising.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, Class Dojo, Basecamp, WhatsApp and Instant Messenger) must be professional in tone and content. No personal information on children should be shared on WhatsApp.
- Personal email addresses, text messaging or public chat / social networking programmes must not be used to communicate with parents. In the event of a communication being made through staff personal accounts staff must clearly state this means of communication is not appropriate and direct parents/carers to email their concerns to either admin@svps1.com or safeguarding@svps1.com or, if appropriate use Class Dojo or Tapestry.
- Whole class or group email addresses will be used throughout the school.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

How will email be managed?

- Email accounts are provided by G-Suite and Office 365.
- Pupils have a G-Suite account to use to access Google Classroom.
- Staff will only use official school accounts to communicate with pupils and parents/carers.
- The forwarding of chain messages is not permitted.

Website and Newsletters

Permission is sought from parents, when they arrive at the school, before uploading photographs of their children on the school website and Sherwell Valley Social Networking Sites. Children's first names and classes are to be used instead of full names.

How will social networking, social media and personal publishing be managed?

- Parents and teachers need to be aware that the internet has emerging online spaces, apps and social networks which allow individuals to publish unmediated content.

- Social networking sites can connect people with similar or even very different interests.

- Users of such sites can be invited to view personal spaces and leave comments, over which there may be limited control. We do not allow children to use such sites at school, and parents are reminded to monitor home usage.

- Although primary age pupils should not use Facebook, Instagram, Tik Tok Snapchat or similar sites, we know that nationally, a significant percentage do. Pupils will be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published and their privacy settings.

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email and Instant Messaging addresses, full names of friends/family, specific interests and clubs etc. This may vary for older children in the school who set up accounts for age appropriate online resources, as email addresses are needed for this.

- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present. This message is shared annually with staff.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat-rooms, instant messenger and many others.
- All staff are encouraged to maintain a professional digital footprint/profile.
- The school uses Facebook, Instagram and Twitter as a source of engagement.

How will filtering and monitoring be managed?

- Filtering is managed by Sophos XG210 which falls in line with government recommendations.
- The school has a filtering and monitoring checklist to mitigate risks of inappropriate activities.
- The school will work with Sophos to ensure that filtering policies are continually reviewed.
- The school has a procedure for monitoring filtering for potential access to banned sites. The Sophos Firewall generates weekly reports listing User Threat Quotient scores for each user.
  All members of the school community will be aware of this procedure.
- The school has a procedure for reporting breaches of filtering. If staff or pupils discover unsuitable sites, such as pornography, radicalisation, suicide, weapons etc they must report the website address (URL) to the ICT team, who records the incident and escalates the concern as appropriate e.g. filter the website.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Patterns and behaviours of students are identified by the ICT team in the weekly Search Reports, such as pornography, radicalisation, suicide, weapons etc. Any concerns must be reported to the Headteacher/DSL and escalated as appropriate.

Technical – Infrastructure & Equipment

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Access rights and filtering are mainly defined by user profiles: Staff (admin, teachers, teaching assistants), pupils, guest users & administrators.

Some devices e.g. iPads may have access for staff to use YouTube (filtered for pupil use) to enhance teaching and learning. These devices are recorded in the Sophos XG210 filtering system and the Weekly Online Monitoring / Filtering Report.

- Children in Years 4, 5 and 6 will be provided with an individual username and individual password; children in Year 3 will initially have an individual username and a class password, the latter being changed to an individual password by Term 2. Children in Year 1 initially use a class username and password which is changed to an individual username with a class password as ability improves.

Children in year 2 will be provided with an individual username and a class password; children in Reception will use a shortened username and class password. As their skills and confidence improve they will have an individual username but a generic class password. Nursery pupils have a *class* username and no password. If required, Guest Users will be allocated an appropriate username and password with no access to shared drives.

- There is a protocol for children to access Google Classroom - this is an email address which is unique to each child. This log-in details, email address AND PASSWORD is sent to parents securely. The password will be changed every September by the ICT team.
- The ICT Manager will keep an up to date record of all usernames and passwords, these are stored and shared in the Google Shared Drive.
- The "master / administrator" passwords for the school ICT system, used by the ICT Manager and ICT support must also be available to the Headteacher and kept in the school safe.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the ICT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and agreed by the Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Manager and Headteacher. If the request is agreed, this action will be recorded.
- An appropriate system is in place for users to report any actual / potential online safety incident to the DSL and ICT team. Initial reporting MUST be through CPOMs, unless the child is at risk of significant harm where you must report the incident immediately to the DSL. Where necessary, an online safety incident report form is completed (Appendix B). This will be displayed on the Safeguarding board.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.
- In the event of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system, "guests" will be allocated a profile which is appropriate for their usage requirements.
- The ICT and internet Policy is in place regarding the extent of personal use that staff are allowed on devices and other portable devices that may be used out of school.
- The ICT and internet policy is in place to inform users regarding the use of removable media (e.g. external HDDs, memory sticks / CDs / DVDs / cameras / memory cards / video cameras / any other USB devices) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software provided by Sophos.

How will Online Safety Safeguarding concerns be handled?

All staff record online safety concerns on CPOMS. The Headteacher, Designated Safeguarding Lead (and Deputies) and any linked members of staff are alerted to these incidents and add the necessary actions to resolve them. Strong communication links are maintained between all staff to ensure incidents are acted upon with immediate effect. The Headteacher reviews all Online Safety concerns on a regular basis.

How will Cyber-Bullying be managed?

Sherwell Valley aims to promote a culture of confident, responsible users of ICT, so that pupils and staff are safe and responsible online. Cyber-bullying (along with all other types of bullying) will not be tolerated. All Online Safety Safeguarding incidents & concerns will be recorded on CPOMS by staff members, using the Online Safety tab button. Staff will specifically state the concern. The necessary adults (parents, teachers, Headteacher) will communicate effectively to help the child resolve the problem. The Designated Safeguarding Lead will also be informed of any Online Safety incidents involving Child Protection concerns and will be escalated appropriately.

For any concerns, please refer to Appendix A

Appendix A

Responding to an Online Safety Concern

Designated Safeguarding Lead (s):

Cristy Nelson, 01803 613292
mrs.nelson@svps1.com

Online Safety Lead: Cristy Nelson

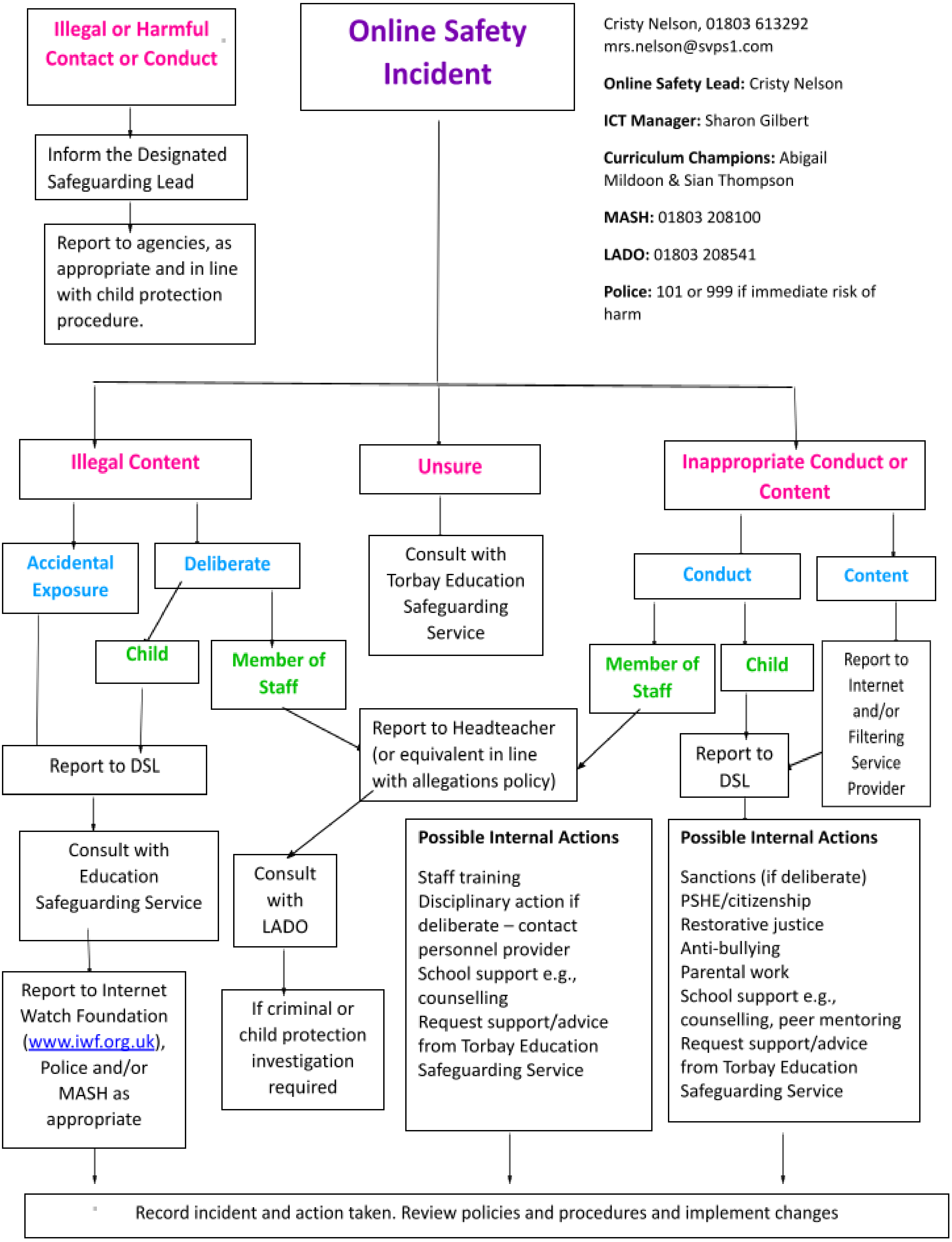
ICT Manager: Sharon Gilbert

Curriculum Champions: Abigail Mildoon & Sian Thompson

MASH: 01803 208100

LADO: 01803 208541

Police: 101 or 999 if immediate risk of harm



Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

Online Safety Incident

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Report to Internet Watch Foundation (www.iwf.org.uk), Police and/or MASH as appropriate

Unsure

Consult with Torbay Education Safeguarding Service

Report to Headteacher (or equivalent in line with allegations policy)

Consult with LADO

If criminal or child protection investigation required

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

Staff training
Disciplinary action if deliberate – contact personnel provider
School support e.g., counselling
Request support/advice from Torbay Education Safeguarding Service

Possible Internal Actions

Sanctions (if deliberate)
PSHE/citizenship
Restorative justice
Anti-bullying
Parental work
School support e.g., counselling, peer mentoring
Request support/advice from Torbay Education Safeguarding Service

Record incident and action taken. Review policies and procedures and implement changes

Appendix B

Online Safety Incident Report Form

This form needs to be attached to the incident logged on CPOMs.

Name of person reporting incident:

Role:

Name of person responsible for acting on this report:

Role:

Details of incident:

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify

Name(s) of staff/pupil concerned:

Date happened:

Time:

Where did the incident occur?

□ In school/service setting □ Outside school/service setting

Type of incident:

□ bullying or harassment (cyber bullying

□ deliberately bypassing security or access

□ hacking or virus propagation

□ prejudice - racist, sexist, LBGT+ phobic, religious hate material

□ terrorist material

□ online sexual grooming

□ online radicalisation

□ child abuse images

□ on-line gambling

□ soft core pornographic material

□ illegal hard core pornographic material

□ other (please specify)

Description of incident:

Nature of incident:

□ **Deliberate access**

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyber bullying□ breach of AUP

□ **Accidental access**

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Action taken:

□ **Staff**

□incident reported to head teacher/Chair of Governors

□advice sought from LADO

□referral made to LADO

□incident reported to police

□ incident reported to Internet Watch Foundation

□ incident reported to IT

□ disciplinary action to be taken

□ online safety policy to be reviewed/amended

□ **Child/young person**

□ incident reported to head teacher/Safeguarding Team

□ advice sought from Torbay Education Safeguarding Service (TESS)

□ referral made to Children's Safeguarding and Social Work (MASH)

□ incident reported to police

□ incident reported to social networking site

□ incident reported to IT

□ child's parents/carers informed

□ disciplinary action to be taken

□ child/young person debriefed

□ online safety policy to be reviewed/amended

□ Racist incident form completed and sent to LA

Outcome of incident/investigation:

Please detail any specific action taken (ie: removal of equipment)

Signed:

Dated: