Dr South's CE Primary School

Bletchingdon Road, Islip, Kidlington, Oxon OX5 2TQ

Faith, Hope and Love

Headteacher: Mr Huw Morgan **Telephone** (01865) 372323
E-mail: office.3655@dr-souths.oxon.sch.uk **Website:** www.dr-souths.co.uk

E-safety Policy (non-statutory)

The Governors at Dr South's CE Primary School adopt the attached E-safety Policy (based on the ODST Model Policy).

Adopted by the Finance, Premises and Personnel Committee in March 2018

Signed ……………………………..…….. **Chair of Finance, Premises and Personnel Committee**

Signed ………………………………………………………………………… **Headteacher**

Review date: March 2020

Review frequency: every two years

Review approval: Finance, Premises and Personnel Committee

Original document	Author DC	V1 draft	18/8/17
Amended	Internal Officer Scrutiny	V1.1 DRAFT	1/9/17
FINAL document	Full Board (adopted)	FINAL	17/10/17

Online Safety Policy Guidance

4	ODST Policy Guidance (Schools may use this to inform the drafting of their non-statutory policy)

I STATEMENT OF INTENT

ODST is committed to the use of computer technologies and recognise access to the internet as a valuable tool for learners of all ages. The internet is increasingly providing the focal point of educational content within the UK. However, trustees recognise that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils.

We are clear that all pupils should use computer facilities, including the internet, as an essential part of the planned curriculum and as a natural part of the modern learning opportunities within our schools. However, we expect schools to educate our pupils about E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom.

II INTRODUCTION

The ODST Policy and guidance for its schools has used the policy templates and assistance issued and updated by the South West Grid for Learning Trust. The SWGfL is an educational trust with an international reputation in supporting schools with online safety and a commitment to provide educational establishments with safe, secure and reliable teaching & learning resources and services.

SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety). Additional information about its services for schools can be found on the SWGfL website – www.swgfl.org.uk

This policy is not a statement of prescribed policy content or style which is a devolved responsibility of the local governing body. It is however a reminder of the statutory and advisory content of any such policy.

III OBJECTIVES

Our Online Safety Policy Guidance is based on the key principles under which our schools

- ensure pupils' internet use and access is appropriate and controlled.
- preventing misuse of internet connected devices.

- ensuring pupils and parents/carers are educated on the risks carried with internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online
- ensuring procedures and access is effectively managed to minimise risks

IV SCOPE

This policy applies to all members of the ODST trust community including staff, pupils, volunteers, parents /carers, visitors, and other users of our schools and sites.

The Education and Inspections Act 2006 empowers Headteachers / Principals 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 E-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 policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

- Governing Body ✓
- Teaching Staff ✓
- Headteacher ✓
- Support staff ✓
- All School Staff ✓
- Pupils ✓
- Parents/carers ✓

V RELEVANT LEGISLATION

It is recommended that legal advice is sought from officers in ODST in the advent of an e safety issue or situation.

- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994.
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978

- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015

VI RELATED POLICIES

- ODST and School Safeguarding & Child Protection Policy
- ODST Equality Policy
- ODST Tackling Extremism and Radicalisation Policy
- School Anti-Bullying Policy
- Data Protection Policy

VII GENERAL PRINCIPLES

Definitions

- Where the term “relevant body” has been used this refers to the Board of Trustees of ODST;
- Unless indicated otherwise, all references to “school” include both schools and academies;
- Unless indicated otherwise, all references to “teacher” include the headteacher;
- Unless indicated otherwise, all references to ‘staff’ include teaching and support staff.
- The term E-Safety refers to all aspects of the taught and untaught curriculum and in the home, where children and young people communicate using electronic media, fixed and mobile devises which have access to the internet. It focuses on ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

VIII DELEGATION

The relevant body has chosen to delegate its functions to local governing bodies and headteachers as set out in this policy

IX MONITORING & EVALUATION

The Local Governing Body and headteacher will monitor the operation and effectiveness of the school’s Behaviour Policy and deal with any queries relating to it. The relevant body, through the ethos committee, will monitor any concerns or complaints raised in relation to the policy on an annual basis

X DATE OF REVIEW

The policy will be reviewed as required by the Board of Trustees of ODST to take account of any legislative changes and / or national policy development as well as feedback from ODST staff and schools and in any event, by 31 July 2021 at the latest.

Trustees will monitor the impact of their policy using:

- Logs of reported incidents
- Annual returns to local Trustees of Children's Services which require statements about on-line safety and policy
- Visits from ODST advisers where safeguarding and E-safety are a feature
- Mmonitoring logs of internet activity (including sites visited) overseen and recorded by LGBs
- Regular updates of guidance for LGBs and the use of self-evaluation/review tools
- Reports to trustee meetings on the topic

XII ROLES AND RESPONSIBILITIES

Governors & Board of Trustees:

- Trustees are responsible for providing guidance and setting expectations for E-safety policy across ODST schools.
- Governors have devolved responsibility for the approval of their E-safety Policy and for reviewing the effectiveness of their policies.

This will be carried out by both Governors & Trustees receiving regular information about E-safety incidents and monitoring reports. ODST would expect a member of the Local Governing Body (LGB) to take on the role of E-safety Governor which may be combined with that of the Child Protection / Safeguarding Governor.

The role of the E-safety Governor will include:

- regular meetings with the E-safety Co-ordinator
- regular monitoring of E-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant LGB and trust committees

Headteachers and Senior Leaders**:**

Trustees expect Headteachers and senior leaders to:

- have a duty of care for ensuring the safety (including E-safety) of all members of the school community.
- be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- ensure that the relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role

- ensure that the managed service provider carries out the E-safety measures that would otherwise be the responsibility of the school technical staff having been made aware of the school's E-safety policy and procedures.)

Teaching and Support Staff

ODST employees should ensure:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher investigation & action
- all digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-safety and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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.

Designated Safeguarding lead (DSL)

ODST would urge LGBs to ensure their DSL is trained in E-safety issues and is aware of the potential for serious 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
- cyber-bullying

Pupils:

ODST is clear that pupils have a role to play in ensuring that their learning is supported by the safe and secure use of the internet, new technologies and mobile devices. to remain both safe and legal when using the internet, they will need to understand the appropriate behaviours and critical thinking skills and show they:

- are responsible for using the school digital technology systems in accordance with the school's Acceptable Use Policy
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- know and understand policies on the use of mobile devices and digital cameras.
- know and understand policies on the taking/use of images and on cyber-bullying at an age appropriate level.
- understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

ODST believes that Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Trustees would urge schools to take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Virtual Learning Environments (VLE) and information about national / local E-safety campaigns / literature.

ODST would expect parents and carers to be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Community / Other Users

Community and other users who access our schools' systems will be expected to sign a Community User Acceptable Use Agreement (AUA) before being provided with access to school systems. (A Community Users AUA Template can be found in the appendices.)

1. Pupils

1.1. The education of pupils in E-safety is an essential part of the school's curriculum provision. ODST believes children and young people need the help and support of our schools and a well-planned curriculum to recognise and avoid E-safety risks and build their resilience.

1.2. Trustees expect E-safety to be a focus in all areas of the curriculum and for all staff to reinforce E-safety messages across the curriculum. Governors are urged to ensure that the E-safety curriculum for their school is broad, relevant and provides progression, with opportunities for creative activities. Trustees would expect LGBs to provide this in the following ways:

- A planned E-safety curriculum as part of Computing/IT, PHSE and other lessons and should be regularly revisited
- Key E-safety messages reinforced as part of a planned programme of assemblies and tutorial and pastoral activities
- Pupils taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils taught to respect copyright when using material accessed on the internet
- Pupils helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff acting as good role models in their use of digital technologies, the internet and mobile devices
- Pupils 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.
- Staff being vigilant in monitoring the content of the websites the young people visit.
- Where pupils research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

2. Parents / Carers

2.1. Trustees are clear that an understanding of E-safety risks and issues is not a reliable skill set for parents and carers but are clear that they play an essential role in the education of their children and in the regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Trustees would urge schools to provide information and awareness to parents and carers through a range of communications and sources of advice and support. This may include:

- Letters, newsletters, web site, VLE
- Parents / Carers information sessions
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant E-safety web sites / publications for example www.saferinternet.org.uk ; http://www.childnet.com/parents-and-carers

3. The Wider Community

3.1. The school may provide opportunities for local community groups or members of the community to gain from the school's E-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-safety
- E-safety messages targeted towards grandparents and other relatives as well as parents.
- The school website providing E-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their E-safety provision

4. Volunteers

4.1. ODST is clear of the essential part that staff E-safety training has in the understanding volunteers have of their responsibilities, as outlined in this policy and in their subject knowledge in being able to deliver a safe curriculum. Trustees would urge all schools to offer comprehensive and regular training, induction and updates and for E-safety to feature in the schools monitoring work. As a minimum ODST would expect:

- E-safety to be a feature of induction programmes for new employees ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- A planned programme of formal E-safety training to be made available to staff with regular updates and reinforcement.
- An audit of the E-safety training needs of all staff will be carried out annually.

4.2. In addition, governors should consider:

- Ensuring their E-safety Coordinator receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations through headteacher reports and reports from the E-safety Coordinator.
- The E-safety policy and its updates are presented to and discussed by staff in staff meetings and INSET days.

- The E-safety Coordinator / Officer provides advice, guidance and training to individuals as required.

5. Governors

5.1. ODST would expect its governors to take part in E-safety training, with particular importance for those who are members of any subcommittee involved in technology, E-safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by external organisations
- Participation in school training sessions for staff or parents (this may include attendance at assemblies / lessons).

6. Technical – infrastructure equipment, filtering and monitoring

6.1. Most ODST schools have a managed ICT service provided by an outside contractor. ODST is clear that it is the responsibility of the LGB to ensure that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the trust's and school's E-safety Policy and the agreed Acceptable Use Agreements.

6.2. It is the devolved responsibility for LGBs to ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented. It will also need to ensure that the relevant people are effective in carrying out their E-safety responsibilities:

6.3. A more detailed Technical Security Policy Guidance can be sourced from the trust, however, Trustees are clear that in ODST schools:

- School / Academy technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)

- A named individual is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages and different groups of users – staff, pupils, parents etc.)

6.4. Trustees would also expect teaching about the responsibilities of internet use to include an awareness that

- School technical staff regularly monitor and record the activity of users on the school technical systems
- A system is in place for users to report any technical incident or security breach to the relevant person.
- Security measures to protect the school's system from accidental or malicious attempts to access the school's systems and data.
- the extent of personal use that users and their family members are allowed on school devices
- the use of removable media (e.g. memory sticks) by users on school devices
- the encryption or otherwise of secured and personal data.

7. Bring Your Own Device (BYOD)

7.1. Trustees are aware of the educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of E-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and trustees would expect LGBs considering allowing this to have their own and separate BYOD policy.

8. Use of digital and video images

8.1. ODST is aware that the development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may

- provide avenues for cyberbullying to take place
- remain available on the internet forever
- cause harm or embarrassment to individuals in the short or longer term.

8.2. ODST expects the school to inform and educate users about these risks and to implement policies to reduce the likelihood of the potential for harm:

8.3. When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

8.4. Trustees have devolved responsibility to LGBs to describe their policy on the taking and storage of images but ODST would expect any such decision to follow school policies concerning the sharing, distribution and publication of those images. Images of children in school should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.

8.5. ODST recognises the guidance from the Information Commissioner's Office on the taking of videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). However, individual LGBs will consider and publish their specific stance on this. Should schools decide to allow this, trustees would expect such policies to respect the privacy and in some cases protection of individuals and be clear that any such images should not be published or made publicly available on social networking sites. Parents/carers should also be warned about making comment on any activities involving other pupils in the images.

8.6. In considering their policy on pupil images LGBs are expected to consider:

- pupil-taken images and their publication or distribution
- photographs published on the website, or elsewhere
- the identification by name a website or blog, particularly in association with photographs.
- the stance on written permission from parents or carers
- the publication or use of pupils' work

9. Data Protection

9.1. 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.

9.2. ODST is also aware that the above act will be superseded in April 2018 by the General Data Protection Regulation (GDPR). Further guidance and training will be available to ensure that our schools are complaint with this statute.

9.3. ODST has its own data Protection Policy[1] and trustees expect each school to hold and review their own policy.

10. Communication & Mobile Technology

10.1. ODST has devolved to school local governing bodies and their unique settings the decisions on the use of mobile technologies. However, it would urge schools to consider carefully their stance on, for example, mobile phones. Trustees recognise that this decision is influenced by the age of the pupils and the following table highlights the decisions ODST expects LGBs to make regarding this area.

[1] https://secure.toolkitfiles.co.uk/clients/26519/sitedata/Vacancies/Data-Protection-Policy-and-Procedures.pdf

	Staff and other Adults				*Students / 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	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras		x						x
Use of other mobile devices e.g. tablets, gaming devices	x							x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails				x				x
Use of messaging apps				x				x
Use of social media				x				x
Use of blogs				x				x

11. Social Media - Protecting Professional Identity

11.1. With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential.

11.2. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012' and in the ODST Staff Conduct Policy.

11.3. All schools and Multi Academy Trusts (MAT) have a duty of care to provide a safe learning environment for pupils and staff. They could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or MAT liable to the injured party, and/or may be subject to criminal and internal disciplinary procedures.

11.4. Trustees would therefore expect reasonable steps to prevent predictable harm to be put in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information and to include:

- Training on: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

11.5. The trust's staff conduct policy reinforces that:

- No reference should be made in social media to pupils, parents/carers or other school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or ODST

11.6. School's use of social media for professional purposes will be checked regularly by the Operations Manager and other officers of ODST

12. Unsuitable / inappropriate activities

12.1. Certain types of internet activity e.g. accessing child abuse images, cyber bullying and distributing racist material is illegal and is therefore not permitted in ODST schools and on ODST technical systems. Such action could lead to criminal prosecution.

12.2. In addition there are a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

12.3. Trustees believe that the activities referred to below, would be inappropriate in a school context or, in some cases risk disclosing personal passwords and bank details on open school systems and that users should not engage in these activities when using school equipment:

- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files

- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (non-educational)
- On-line gambling
- File sharing
- Use of messaging apps

Responding to incidents of misuse

12.4. 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.

Illegal Incidents

12.5. 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 in Appendix A for responding to online safety incidents and report immediately to the police.

Other Incidents

12.6. ODST expects all members of the school community to be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

12.7. **In the event of suspicion, ODST expects its senior leaders and governors to act promptly and to take all the steps in this procedure:**

- Have more than one senior member of staff and/or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation 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.
- Ensure during the investigation that the sites and content visited are closely monitored and recorded (to provide further protection); recording the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may 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 record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the individual 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 ODST officers or national/local organisations (as relevant).
    - Police involvement and/or action
- **If the 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
    - 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.**

12.8. It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form (see appendix G) should be retained by the investigating panel for evidence and reference purposes.

13. School Actions & Sanctions

13.1. It is more likely that our schools will 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 pupils are aware of the standards in place to minimise any breaches. It is expected that incidents of misuse will be dealt with through normal behaviour policies and procedures. However, Trustees would urge governors to consider the following issues in their behaviour and sanctions procedures:

- Deliberately accessing or trying to access material that could be considered illegal (
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone, digital camera and/or other mobile device
- Unauthorised use of social media/messaging apps or personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another pupil's account or the account of a member of staff
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Accidentally accessing offensive or pornographic material and failing to report the incident

- Deliberately accessing or trying to access offensive or pornographic material

13.2. Trustees are aware that staff conduct policies may need to recognise and reflect similar infringements by adults, employees and volunteers and will keep such ODST policies under review.

14. Other Associated Polices

14.1. Governors may wish to consider other associated policies which impact on the provision of IT in schools. Governors may seek support from ODST in framing these policies. These include:

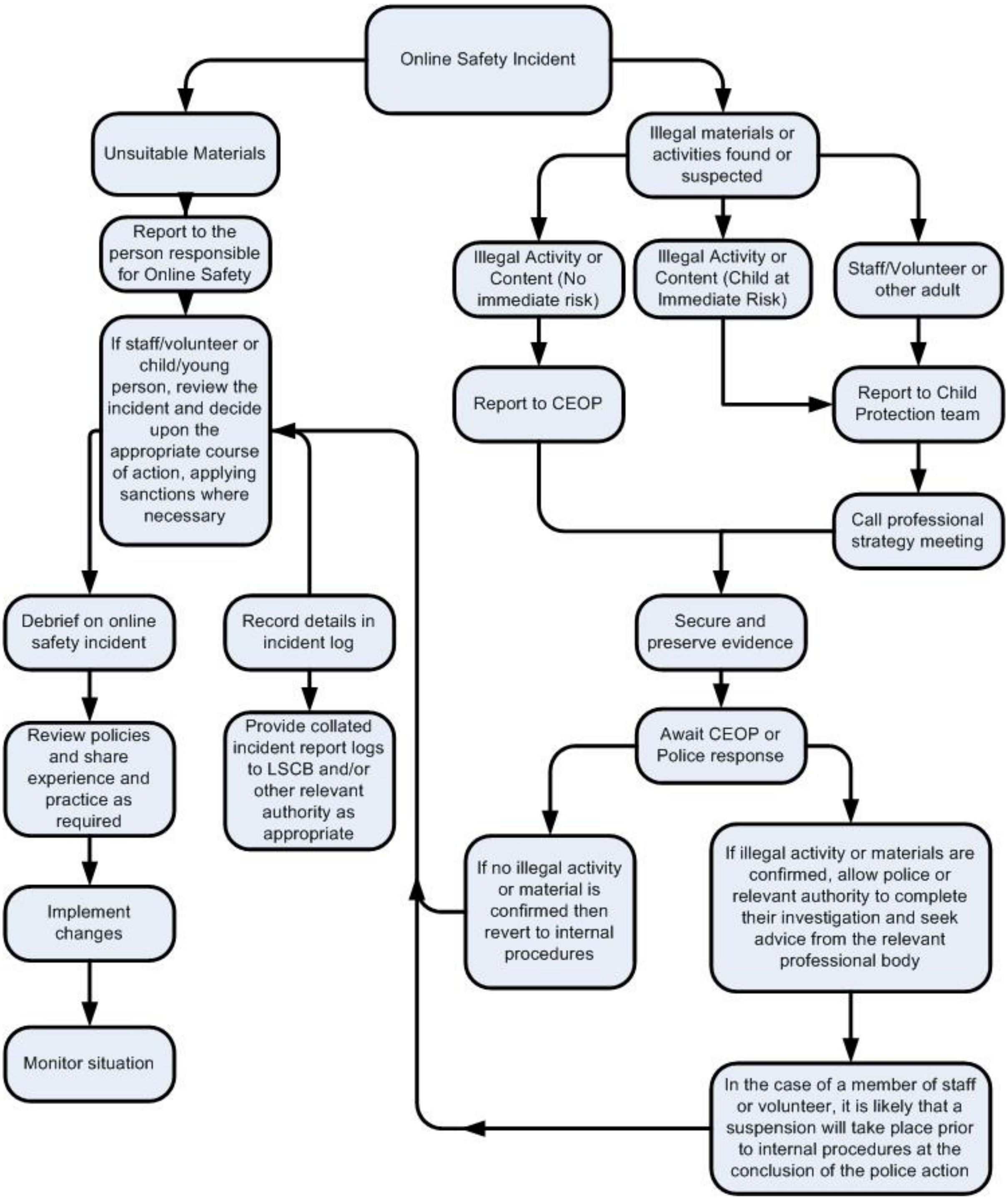
- Technical Security Policy (including filtering and password)
- Personal Data Handling Policy
- Electronic Devices - Searching & Deletion
- Mobile Technologies Policy
- Social Media Policy

And the use of a governors' on-line safety group with

- Online Safety Group Terms of Reference

Appendix A

Responding to incidents of misuse – flow chart


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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Appendix B

Responding to incidents of misuse – record form

Date: ....

Reason for investigation: ....

....

....

....

<u>Details of first reviewing person</u>

Name: ....

Position: ....

Signature: ....

<u>Details of second reviewing person</u>

Name: ....

Position: ....

Signature: ....

Name and location of computer used for review (for web sites)

....

....

Web site(s) address / device	Reason for concern

Reporting Log

Group: ....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Conclusion and Action proposed or taken

Links to other organisations or documents

The following links may help those who are developing or reviewing school online safety policies:

- UK Safer Internet Centre
- Safer Internet Centre – http://saferinternet.org.uk/
- South West Grid for Learning - http://swgfl.org.uk/
- Childnet – http://www.childnet-int.org/
- Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
- Internet Watch Foundation - https://www.iwf.org.uk/
- CEOP - http://ceop.police.uk/
- ThinkUKnow - https://www.thinkuknow.co.uk/

Others

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - http://www.netsmartz.org/

Tools for Schools

- Online Safety BOOST – https://boost.swgfl.org.uk/
- 360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

- Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
- DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
- Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
- Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

- Digizen – Social Networking
- UKSIC - Safety Features on Social Networks
- SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- SWGfL Digital Literacy & Citizenship curriculum
- Glow - http://www.educationscotland.gov.uk/usingglowandict/
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Mobile Devices / BYOD
- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN   - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

- Your rights to your information – Resources for Schools - ICO
- Guide to Data Protection Act - Information Commissioners Office
- Guide to the Freedom of Information Act - Information Commissioners Office
- ICO guidance on the Freedom of Information Model Publication Scheme
- ICO Freedom of Information Model Publication Scheme Template for schools (England)
- ICO - Guidance we gave to schools - September 2012 (England)
- ICO Guidance on Bring Your Own Device
- ICO Guidance on Cloud Hosted Services
- Information Commissioners Office good practice note on taking photos in schools
- ICO Guidance Data Protection Practical Guide to IT Security
- ICO – Think Privacy Toolkit
- ICO – Personal Information Online – Code of Practice
- ICO Subject Access Code of Practice
- ICO – Guidance on Data Security Breach Management
- SWGfL -   Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

- NEN - Guidance Note - esecurity

Working with parents and carers

- SWGfL Digital Literacy & Citizenship curriculum
- Online Safety BOOST Presentations - parent's presentation
- Connectsafely Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops / education
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- The Cybersmile Foundation (cyberbullying) - advice for parents

Research

- EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
- Futurelab - "Digital participation - its not chalk and talk any more!"
- Ofcom – Children & Parents – media use and attitudes report - 2015