Oxford Diocesan Schools Trust
St Mary's Convent
Denchworth Road, Wantage
Oxford, OX12 9AU
01865 208286
odst.governance@oxford.anglican.org
www.odst.org.uk

Statutory Policy:	Policy provided centrally for adoption by schools with minimal amendment to the core text. Changes are allowed to the text where indicated

Online Safety & Acceptable Use of Information & Communications Technology (ICT) Policy

St Peter's CE Middle School, Old Windsor

Approved by:	**Estates & Safeguarding**
Date:	**May 2023**
Next review date:	**July 2026**

Adopted by school:	**SPMS Governors**
Date:	**25th September 2024**

Contents

Statement of Intent

ODST is committed to the use of computer technologies and recognises 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.

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 Safety and Security Online | SWGfL .
This policy is not a statement of prescribed policy content or style which is a devolved responsibility of the Local Governing Body (LGB). It is however a reminder of the statutory and advisory content of any such policy.

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.

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 and Behaviour Principles Written Statement.

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.

Local Governing Body	✓
Teaching Staff	✓
Headteacher	✓
Support staff	✓
All School Staff	✓
Pupils	✓
Central Office Staff	✓
Parents/carers	✓
Contractors/Service Providers	✓
Users of the school site and buildings	✓

Relevant Legislation

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

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Telecommunications Act 1984
- Public Order Act 1986
- Malicious Communications Act 1988
- Data Protection Act 2018
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Trademarks Act 1994
- Criminal Justice & Public Order Act 1994
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Communications Act 2003
- Sexual Offences Act 2003
- The Education and Inspections Act 2006
- Racial and Religious Hatred Act 2006
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015

- Protection from Harassment Act 1997
- Protection of Children Act 1999
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)
- GDPR (General Data Protection Regulation) 2018
- Telecommunications (Security) Act 2021
- Searching, screening and confiscation: advice for schools 2023

Related Policies

- ODST and School Safeguarding & Child Protection Policy
- ODST Behaviour Principles Statement and Schools' Behaviour Policies
- ODST Equality Policy
- ODST Tackling Extremism and Radicalisation Policy
- School Anti-Bullying Policy
- Data Protection Policy
- Governors Code of Conduct
- Staff Code of Conduct

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.

Delegation

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

Monitoring & Evaluation

The Local Governing Body and Headteacher will monitor the operation and effectiveness of this Policy and deal with any queries relating to it. The relevant body, through the Ethos & Governance Committee, will monitor any concerns or complaints raised in relation to the policy on an annual basis.

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 2025** 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
- monitoring 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.

Roles and Responsibilities

General:
All schools must review their practice against the standards below.

Governors & Board of Trustees:

- Trustees are responsible for providing guidance and setting expectations for E-safety policy across ODST schools. ODST urges all schools to read and ensure that their practice adheres to the standards in www.gov.uk 2023; Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK
- 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 E-safety Co-ordinator and other 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
- receive regular monitoring reports from the E-safety Co-ordinator / Officer
- 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.

E-safety Coordinators
Trustees strongly recommend that each school should have a named member of staff with a day to day responsibility for E-safety. They will:

- take day to day responsibility for E-safety issues and a leading role in establishing and reviewing the school E-safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- provide training and advice for staff
- liaise with external bodies
- report on E-safety incidents to the Senior Leadership Team and keep a log of incidents to inform future E-safety developments
- meet regularly with the E-safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meetings of Governors / Trustees.

Teaching and Support Staff
ODST employees should ensure:

- they have an up to date awareness of E-safety matters and of the current Trust and 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.)

Online Safety Policy Guidance

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 about 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.

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 every (insert period). (LGBs may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the associated risks)
  Tthe "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 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 of 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 2018 and the General Data Protection Regulation (GDPR) 2018 which states that personal data must be:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation.

9.2. ODST has its own Data Protection Policy 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.

Communication Technologies	Staff & other adults			Students/Pupils				
	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 mobile phones / cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

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
- On-line shopping/commerce
- 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 F 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:
  on-line safety group terms of reference.

15. Appendices

The following appendices are recommended for adoption alongside the school's E-safety policy and some are referred to in the ODST policy guidance.

Each can be copied onto school headed paper and adjusted to suit the age and stage of pupils or the intended audience.

Appendix A - Pupil Acceptable Use Agreement Form for older pupils (KS2/3)

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
-

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school network, receive other sanctions and my teacher may contact my parents. In the event of illegal activities this may involve the police.

I have read and understand the above and agree to follow these guidelines when I use the *school* systems and devices (both in and out of school)

Name of Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

Signed (parent/carer): (optional) .....

It is for schools to decide whether or not they require parents / carers to sign the Parent/Carer Acceptable Use Agreement (see template appendix C). Some schools may, instead, wish to add a countersignature box for parents / carers to the pupil Acceptable Use Agreement.

Appendix B - Parent / Carer Acceptable Use Agreement – Template A

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As the parent / carer of the named pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

(Schools will need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

Pupil's name: .....

Parent/carer's name: .....

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Appendix C - Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that users are protected from potential risk in their use of these systems and devices.
- Acceptable Use Agreement
- I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school / academy:
- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school / academy has the right to remove my access to school systems / devices
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: .....

Organisation: .....

Signed: .....

Date: .....

Appendix D - Staff (and Volunteer) Acceptable Use Policy Agreement Template

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school / academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school (schools / academies should amend this section in the light of their policies which relate to the use of school systems and equipment out of school)
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school / academy ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website /VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies. (schools / academies should amend this section to take account of their policy on access to social networking and similar sites).
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications).
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules which may be set by the school's Local Governing Body about such use (see section 7). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email.
- I will ensure that my data is regularly backed up, in accordance with school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that General Data Protection Regulations require that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any loss of such data and any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action as set down in Trust HR policies and in the event of illegal activities the involvement of the police.

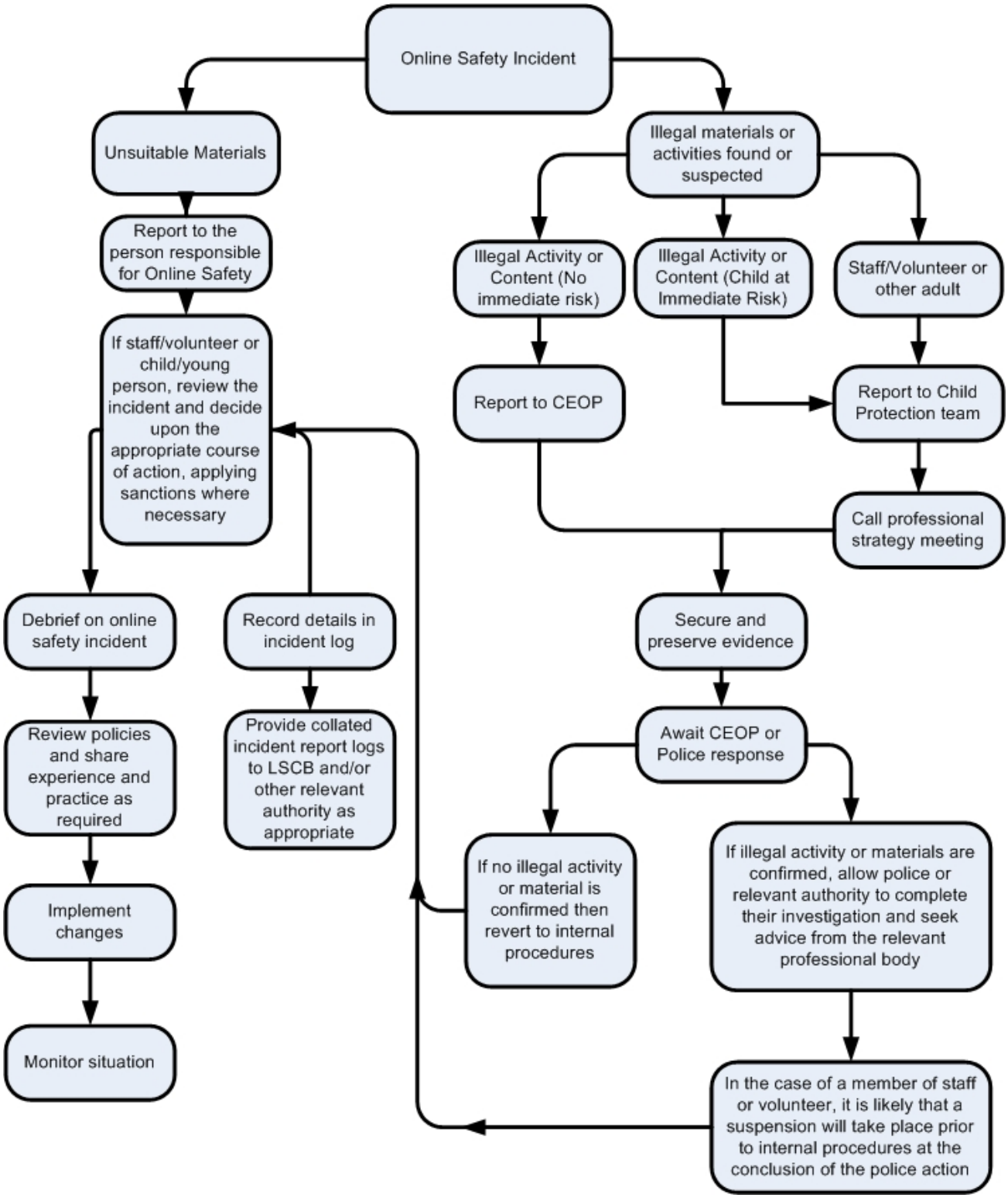
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/volunteer name: .....

Signed: .....

Date: .....

Appendix E - Responding to incidents of misuse – flow chart



Appendix F - Responding to incidents of misuse – record form

Group:	
Date:	
Reason for investigation:	
Details of first reviewing person	
Name:	
Position:	
Signature:	
Details of second reviewing person	
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 and documents

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

- UK 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
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- http://swgfl.org.uk/
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Mobile Devices / BYOD
- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN - http://swgfl.org.uk/

Data Protection

Information Commissioners Office:

- Information Commissioner's Office (ICO)
- Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

- 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

- ICO Guidance Data Protection Practical Guide to IT Security
- ICO – Think Privacy Toolkit

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People in Keeping children safe in education - GOV.UK (www.gov.uk)
- 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)
- 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