Bampton CE Primary School and Nursery

Learning together with Respect, Friendship and Perseverance

School Vision Statement

We endeavour to enable all individuals in our school community to learn together, grow in respect, tolerance and understanding of the world in which we live and embrace Christian values, to be the best that we can be.

Title of Policy	**E-Safety Policy**
Date Adopted by the Governing Body	**January 2022**
Review Date	**January 2023**
Signed by the Chair of Governors	

I STATEMENT OF INTENT

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 ODBST 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 ✓
- Central Office Staff ✓

- Parents/carers ✓
- Contractors/ Service Providers ✓
- Users of the school site and buildings ✓

V RELEVANT LEGISLATION

It is recommended that legal advice is sought from officers in ODBST 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
- Keeping Children safe in Education 2021
- Equalities Act 2010
- Data protection Act 2018

VI RELATED POLICIES

- ODBST and School Safeguarding & Child Protection Policy
- ODBST Equality Policy
- ODBST Tackling Extremism and Radicalisation Policy
- School Anti-Bullying Policy
- Data Protection Policy
- School Technical Security Policy Guidance
- Social Media Policy

VII GENERAL PRINCIPLES

Definitions

- Where the term “relevant body” has been used this refers to the Board of Trustees of ODBST;
- 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 2023 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

Local Governors & Board of Trustees:

- Trustees are responsible for providing guidance and setting expectations for E-safety policy across ODST schools.
- Local 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.)

<u>E-safety Coordinators</u>

Trustees strongly recommended 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*

<u>Teaching and Support Staff</u>

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)

ODBST 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 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 and on-line pupil records

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 should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils taught to respect copyright when using material accessed on the internet
- Pupils helped to understand the need for the 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:

- Curriculum activities
- Letters, newsletters, web site,
- 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 *(see appendix J for further links/resources)*

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. Staff and 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 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 volunteers and staff 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.
- On line safety may feature in some staff performance reviews

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. KS1 and below, have shared passwords.
- 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 securely by TurnITOn, our IT support.
- 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.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- There is a clear process in place to deal with requests for filtering changes (see ODST School Technical Security Policy Guidance 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.) .
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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. Mobile Technologies (including Bring Your Own Device (BYOD))

7.1. Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

7.2. All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

7.3. 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.

7.4. The school allows:

	School Devices			Personal Devices		
Mobile Technologies	**School owned for single user**	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*√*	*√*	*√*		*√*	*√*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Full network access	√	√	√		√	
Internet only						√
No network access						

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. Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press

8.4. 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.

8.5. 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.

8.6. 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.

8.7. In considering their policy on pupil images LGBs are expected to note and include to reduce the likelihood of potential harm:

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

9. Data Protection

9.1. With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, Trustees expect Governors to note the likelihood of greater scrutiny in their care and use of personal data.

9.2. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school/academy must ensure that:

- it has adopted a Data Protection Policy. (see ODST policy)
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed).
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. (The Trust's 'retention policy" applies to the deletion and disposal of data supports this).
- personal data held must be accurate and up to date where this is necessary for the purpose it is processed for withsystems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- it provides staff, parents, volunteers, and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, which enables an individual to see or to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems.

Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- it has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

9.3. When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

9.4. 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. A wide range of rapidly developing communications technologies has the potential to enhance learning. 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.

	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	√							√
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		√						√

10.2. When using communication technologies, the school/academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

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. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way. Trustees would urge LGBs to complete the ODST Social Media Policy Guidance template.

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:

- Ensuring that personal information is not published
- 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 ODBST
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including

- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school/academy disciplinary procedures

11.7. Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

11.8. Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's/academy's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

12. Unsuitable / inappropriate activities

12.1. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Such action could lead to criminal prosecution.

12.2. Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

12.3. 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.

12.4. 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]
- Use of video broadcasting e.g. Youtube

<u>Responding to incidents of misuse</u>

12.5. 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.

<u>Illegal Incidents</u>

12.6. 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 G for responding to online safety incidents and report immediately to the police.

<u>Other Incidents</u>

12.7. 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.

12.8. **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/discriminatory material
    - promotion of terrorism or extremism offences under the Computer Misuse Act (see Appendix G)
    - 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.**

12.9. 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 H) 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 suggested procedures as follows:

These actions are for guidance and will depend on the circumstances and severity of the incident and the age and intention of the perpetrator.	Actions/Sanctions									
Pupils Incidents using school networks or hardware	Refer to class teacher	Refer to Head of Year/phase	Refer to Headteacher	Refer to MAT	Refer to Police	Inform parents/carers	Warning	Removal of network/internet access rights	Further sanction e.g. detention/exclusion	Refer to technical support staff for action re filtering/security etc.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		N/A	X	X	X	X		X	X	X
Unauthorised use of non-educational sites during lessons	X		X			X				X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x		X			X		X		
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x		X			X		X		X
Unauthorised downloading or uploading of files	x		x				X			X
Allowing others to access school/academy network by sharing username and passwords	x		x				X			X
Attempting to access or accessing the school/academy network, using another student's/pupil's account	x		x				X			X
Attempting to access or accessing the school/academy network, using the account of a member of staff			X	X		X	X	X		X
Corrupting or destroying the data of other users			X			X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment, discriminatory or of a bullying nature			X	X		X	X			
Continued infringements of the above, following previous warnings or sanctions			X	X		X	X	X	X	
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school			X			X	X			
Using proxy sites or other means to subvert the school's/academy's filtering system			X					X		X
Accidentally accessing offensive, discriminatory, or pornographic material and failing to report the incident	X			X			X			X

Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X	X		X
Transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X		X		(X)		X

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 ODBST policies under review but notes schools should consider:

These actions are for guidance and will depend on the circumstances and severity of the incident and the age and intention of the perpetrator.	Actions/Sanctions							
Staff Incidents using school networks or hardware	Refer to line manager	Refer to Headteacher Principal	Refer MAT/HR	Refer to Police	Investigation	Suspension	Disciplinary action	Refer to Technical Support Staff for action re filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email	X	X	X		X			
Unauthorised downloading or uploading of files	X							X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X						X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X						X
Deliberate actions to breach data protection or network security rules		X	X		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	(X)	X		X	X
Sending an email, text or message that is regarded as offensive, harassment, discriminatory or of a bullying nature	X	X		X	X			
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	X	X		X	X			
Actions which could compromise the staff member's professional standing	X	(X)						

Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy	X		X		X			
Using proxy sites or other means to subvert the school's/academy's filtering system		X	X	(X)	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X							
Deliberately accessing or trying to access offensive or pornographic material		X	X		X		X	X
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions		X	X		X		X	

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:

- ODST Remote Learning Policy Guidance
- ODST Social Media Policy Guidance (Template)
- ODST Remote Learning Checklist suite
- ODST Safeguarding Policy Annex (updated)
- 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

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.

A. Student/Pupil Acceptable Use Agreement Template – for younger pupils (Foundation/KS1)
B. Student/Pupil Acceptable Use Policy Agreement Template – for older pupils (KS2)
C. Parent/Carer Acceptable Use Agreement Template
D. Staff (and Volunteer) Acceptable Use Policy Agreement Template
E. Acceptable Use Agreement for Community Users Template
F. Staff (and Volunteer) Acceptable Use Policy Agreement Template
G. Responding to incidents of misuse – flow chart
H. Record of reviewing devices/internet sites (responding to incidents of misuse) Reporting Log
I. Social Media Policy Template
J. Links to other organisations or documents

Appendix A

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):…….

Signed (parent): ……

Appendix B

Pupil Acceptable Use Agreement Form for older pupils (KS2)

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: .....

Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature ……

Appendix C

Parent / Carer Acceptable Use Agreement – Template

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

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

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

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.

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.

Parent / Carers Name: .....

Date: .....

Pupil Name:.....

Appendix E

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 F

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.

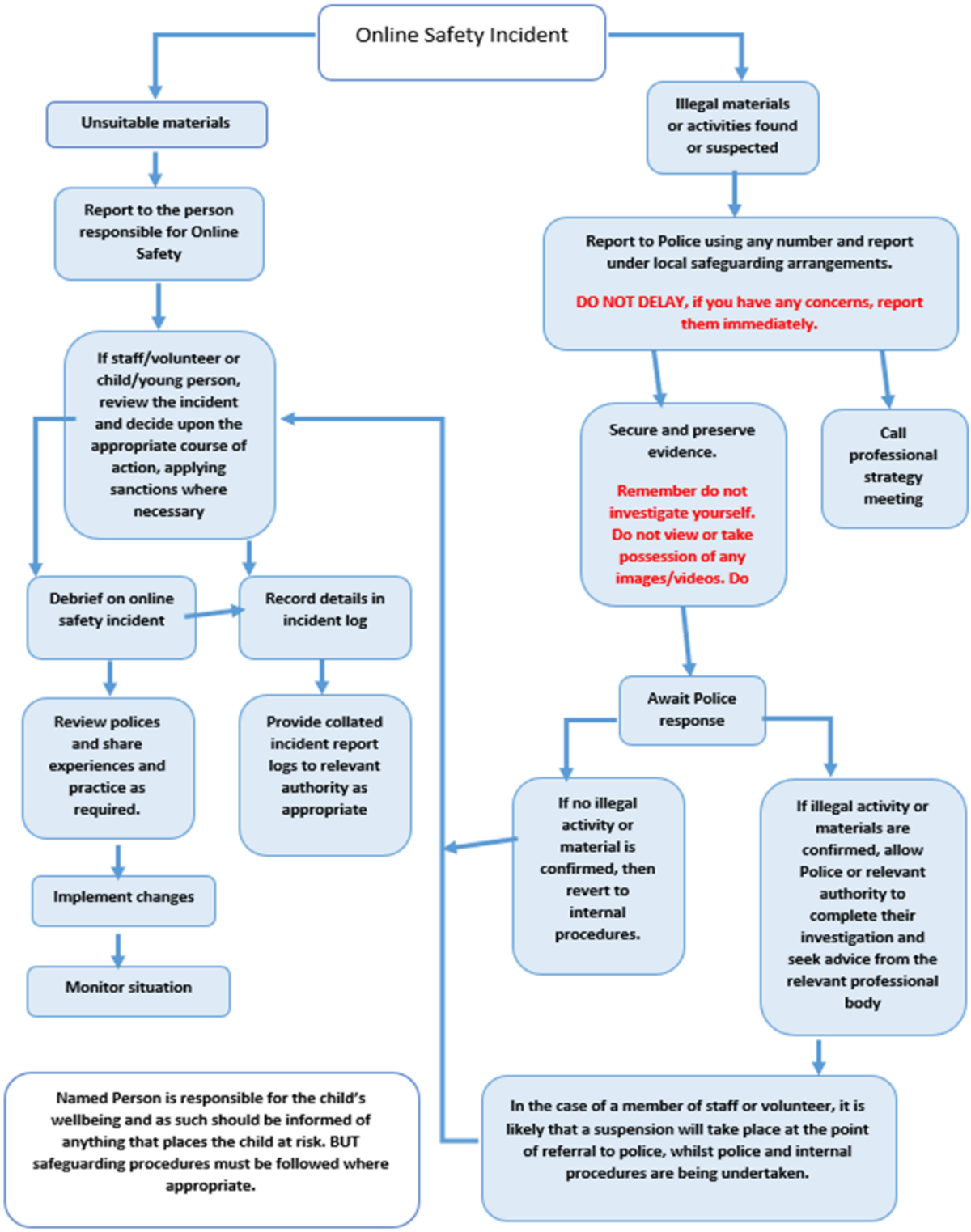
Staff / Volunteer Name: ……..

Signed: …….

Date: ……

Appendix G

Responding to incidents of misuse – flow chart



Appendix H

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

Appendix I

Social Media Policy Guidance

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. Some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube also have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. Our policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

1. Scope

   This policy is subject to the school's and Trust's codes of conduct and acceptable use agreements. It:

   - Applies to all staff and to all online communications which directly or indirectly, represent the school/academy.
   - Applies to such online communications posted at any time and from anywhere.
   - Encourages the safe and responsible use of social media through training and education

   1.1. The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

   1.2. Professional communications are those made through official channels, posted on a school account or using the school/academy name. All professional communications are within the scope of this policy.

   1.3. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

   Personal communications which do not refer to or impact upon the school/academy are outside the scope of this policy.

   1.4. Digital communications with pupils/students are also considered. Staff may use social media to communicate with learners via a professional school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

2. Organisational control

   2.1. Roles & Responsibilities

   - **SLT**
     - Facilitating training and guidance on Social Media use.

- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

- **Administrator/Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school/academy accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school/academy

3. Process for creating new accounts

3.1. The school and Trust is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

3.2. Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school/academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/academy, including volunteers or parents.

4. Monitoring

4.1. School accounts must be monitored regularly and frequently (including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

5. Behaviour

5.1. The school/academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

5.2. **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**.

5.3. School/academy social media accounts must not be used for personal gain.

5.4. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school/academy.

5.5. Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

5.6. If a journalist makes contact about posts made using social media staff must report this to the headteacher who will seek guidance from the Diocesan Media Relations Team before responding.

5.7. Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school/academy and will be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.

5.8. The use of social media by staff while at work may be monitored, in line with school/academy policies.

5.9. The school/academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/academy will deal with the matter internally. Where conduct is considered illegal, the school/academy will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

6. Legal considerations

6.1. Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

6.2. Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

7. Handling abuse

7.1. When acting on behalf of the school/academy, handle offensive comments swiftly and with sensitivity.

7.2. If a conversation turns and becomes offensive or unacceptable, school/academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

7.3. If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school/academy protocols.

8. Tone

8.1. The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational

- Informative
- Friendly (on certain platforms, e.g. Facebook)

9. Use of images

9.1. School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

9.2. Permission to use any photos or video recordings should be sought in line with the school's/academy's digital and video images policy.

9.3. Under no circumstances should staff share or upload student/pupil pictures online other than via school/academy owned social media accounts

9.4. Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Students/pupils should be appropriately dressed, not be subject to ridicule and must not be on any school/academy list of children whose images must not be published.

9.5. If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

10. Personal use

10.1. Staff

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

10.2. Pupils

- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
- The school's education programme should enable the pupils/students to be safe and responsible users of social media.

10.3. Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- Parents/Carers are encouraged to comment or post appropriately about the school/academy. In the event of any offensive or inappropriate comments being made, the school/academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's/academy's complaints procedures.

11. Monitoring posts about the school

11.1. As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school. The school will respond to social media comments made by others according to a defined policy or process.

Appendix 1

Managing school/academy social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Appendix J Links to other organisations or documents

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

- Safer Internet Centre – https://www.saferinternet.org.uk/
- South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
- Childnet – http://www.childnet-int.org/
- Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
- Revenge Porn Helpline - https://revengepornhelpline.org.uk/
- Internet Watch Foundation - https://www.iwf.org.uk/
- Report Harmful Content - https://reportharmfulcontent.com/

CEOP

- CEOP - http://ceop.police.uk/
- ThinkUKnow - https://www.thinkuknow.co.uk/

Others

- LGfL – Online Safety Resources
- Kent – Online Safety Resources page
- INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
- UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
- 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/
- 360Data – online data protection self-review tool: www.360data.org.uk
- SWGfL Test filtering - http://testfiltering.com/
- UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying / Cyberbullying

- Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
- SELMA – Hacking Hate - https://selma.swgfl.co.uk
- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
- 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 – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit: Childnet – Project deSHAME – Online Sexual Harrassment ; UKSIC – Sexting Resources
- Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
- Ditch the Label – Online Bullying Charity
- Diana Award – Anti-Bullying Campaign

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 Evolve - https://projectevolve.co.uk
- UKCCIS – Education for a connected world framework
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources

Data Protection

- 360data - free questionnaire and data protection self review tool
- ICO Guides for Education (wide range of sector specific guides)
- DfE advice on Cloud software services and the Data Protection Act
- IRMS - Records Management Toolkit for Schools
- NHS - Caldicott Principles (information that must be released)
- ICO Guidance on taking photos in schools
- Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

- DfE – Keeping Children Safe in Education (2021)
- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Childnet – School Pack for Online Safety Awareness
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

- UKSIC – Appropriate Filtering and Monitoring
- SWGfL Safety & Security Resources
- Somerset - Questions for Technical Support
- NCA – Guide to the Computer Misuse Act
- NEN – Advice and Guidance Notes

Working with parents and carers

- Online Safety BOOST Presentations - parent's presentation
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops/education
- Internet Matters

Prevent

- Prevent Duty Guidance
- Prevent for schools – teaching resources
- NCA – Cyber Prevent
- Childnet – Trust Me

Research

- Ofcom –Media Literacy Research