Idsall School
E-Safety Policy

Sponsorship & Review

1 Sponsor

Ms D Campbell, Deputy Head
Mr A Groucutt, IT Network Manager

2 Reviewed

January 2023

3 Next Revision Date

January 2024

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by:

- *Headteacher / Senior Leaders*
- *E-Safety Coordinator*
- *IT Network Manager*
- *Trustees*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Contents

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Board / Trustees Sub Committee on:*	January 2022
The implementation of this e-safety policy will be monitored by the:	*Deputy Head with responsibility for E-Safety (E-Safety Coordinator), the IT Network Manager and Senior Leadership Team.*
Monitoring will take place at regular intervals:	*- at least once a year*
E-Safety Group / E-Safety Trustee will receive a report of the e-safety policy generated by the e-safety coordinator at termly meetings	*- at each termly E-Safety group meeting*
The E-Safety Policy will be reviewed every year or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*January 2024*
Should serious e-safety incidents take place, the following persons / agencies should be informed:	*DSL, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity*
- *Surveys / questionnaires of students and staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the *school*:

Trustees:

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Trustees* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Board* has taken on the role of *E-Safety Trustee*. The role of the E-Safety Trustee will include:

- *regular updates from the* E-Safety Co-ordinator at Trustees' meetings
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- **The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures). SWGfL BOOST includes an 'Incident Response Tool' with steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. This can be downloaded at http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This will be done through regular meetings between the e-safety coordinator and the Headteacher.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator

E-Safety Coordinator:

- facilitates the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

- meets regularly with E-Safety Trustee to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Trustees
- reports regularly to Senior Leadership Team

IT Network Manager:

The IT Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the internet filtering, is applied and updated on a regular basis
- that IT Network Manager keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / cloud / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- 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 (AUP)
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / 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
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students 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

Child Protection / Safeguarding Designated Person / Officer

Should be trained in e-safety issues and be 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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and monitoring the e-safety policy, including the impact of initiatives. Depending on the size or structure of the school, this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Board.

Members of the *E-safety Group* will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the e-safety provision
- monitoring improvement actions identified through use of the '360 degree safe' self-review tool

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should 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

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will 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
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in e-safety is, therefore, an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students 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
- Where students are allowed to freely search the internet, staff should be aware of the content of the websites the students visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, abortion, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Support Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable via a IT Helpdesk ticket, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online 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.

The school will, therefore, seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, website*
- *Reference to the relevant websites / publications*

  e.g. *www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- *The school website will provide e-safety information for the wider community*

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff should receive regular e-safety training, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator / IT Network Manager will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Trustees

Trustees should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff.

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed by the IT Network Manager in ways that ensure that the school meets recommended technical requirements based on training, research, conferences and advice from technical providers or the local authority.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling where possible should be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by IT Support staff who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 120 days.
- The IT Network Manager 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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.
- The school has provided enhanced / differentiated user-level filtering e.g. Network Administrators / Staff / KS3 / KS4 / KS5.
- IT support staff, when necessary, monitor and record the activity of users on the school technical systems and users are made aware of this in the ICT Acceptable Use Policy.
- An appropriate system (IT Helpdesk/Email) is in place for users to report any actual / potential technical incident / security breach to the IT Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Provision of temporary access of “guests” (e.g. Cover teachers and visitors) onto the school systems is provided with a temporary username and password issued by IT support staff.

Bring Your Own Device (BYOD)

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 a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the ICT Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- All devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Training regarding BYOD is available for all staff
- Monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students 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. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the General Data Protection Regulation). To respect everyone's privacy, and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.
- 3rd parties e.g. visitors, contractors or visiting sports teams are not permitted to take photos and video.
- Staff 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 unless permission is granted from the SLT line manager. If staff use their own equipment e.g. phone/camera to take images of a school event/trip – the images should be uploaded to the school network at the earliest convenience and then deleted from their personal device.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' surnames will not be used anywhere on a website or blog, particularly in association with photographs or videos.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, blogs or social networking. This permission is collected via a data collection form and stored in SIMS.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 which states that personal data must be:

- Fair and lawful.
- Specific for its purpose.
- Adequate and only for what is needed.
- Accurate and up to date.
- Not kept longer than needed.
- Take into account people's rights.
- Kept safe and secure.
- Not be transferred outside the EEA.

The school must ensure that:

- It will hold 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
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”
- It has a Data Protection Policy (see appendix)
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.
- That data is stored within the EEA unless approved protection standards are in place e.g. Privacy Shield / Safe Harbour

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- If computers are left unattended then the computer logon session should be locked (+ L) to prevent unauthorised access. A screensaver timeout is enforced which will lock the screen.

- Use personal data only on secure password-protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer virus and malware checking software

The data must be securely deleted from the device, in line with school data protection policy once it has been transferred or its use is complete.

Preventing Radicalisation and Extremism – see Appendix U for details

The school's **Child protection policy**, which is available on our website (www.idsallschool.org) and in school, covers Radicalisation and Extremism.

CONTEXT: The internet, in particular social media, is being used as a channel to promote and engage. Often this promotion glorifies violence, attracting and influencing many people including children and in extreme cases, radicalising them. Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it.

This threat is not just from groups, such as Islamic State, but from 'far right' groups also.

Critical risk factors could include:

- Being in contact with extremist recruiters.
- Accessing violent extremist websites, especially those with a social networking element.
- Possessing or accessing violent extremist literature.
- Using extremist narratives and a global ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Joining or seeking to join extremist organisations.

Preventing Violent Extremism

Roles and responsibilities of the Point of Contact (POC); the POCs for Idsall School are Cath Cork (Assistant Headteacher) and Jennie Reeve (Pastoral Lead), who are responsible for:

- Liaising with the Idsall School network manager to ensure that appropriate levels of filtering and monitoring are in place to meet the needs of the school's Safeguarding and Child Protection policies and to meet the needs of the Prevent Strategy.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Acting as the first point of contact within the school for case discussions relating to students/pupils who may be at risk of radicalisation or involved in terrorism.

Communications

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

	Staff & other			Students			
Communication Technologies	Allowed	Allowed with permission	Not Allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	X				X		
Use of mobile phones in lessons for educational use	X						X
Use of mobile phones in lessons for personal use			X	X			
Use of mobile phones in social time	X			X			
Taking photos on personal devices during school trips		X					X
Taking photos on personal devices during lessons			X				X
Taking photos on school mobile phones / tablets /	X				X		
Use of other mobile devices e.g. tablets	X						X
Use of other gaming devices			X	X			
Use of personal email addresses in school e.g. GMail	X				X		
Use of school email for personal emails			X	X			
Use of messaging apps			X	X			
Use of social media		X				X	X
Use of blogs	X						X

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities 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* liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: 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

School staff should ensure that:

- No reference should be made in social media to students, parents / carers or 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior information risk officer and e-safety committee to ensure compliance with the Data Protection (GDPR), E-mail, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts usage as follows:

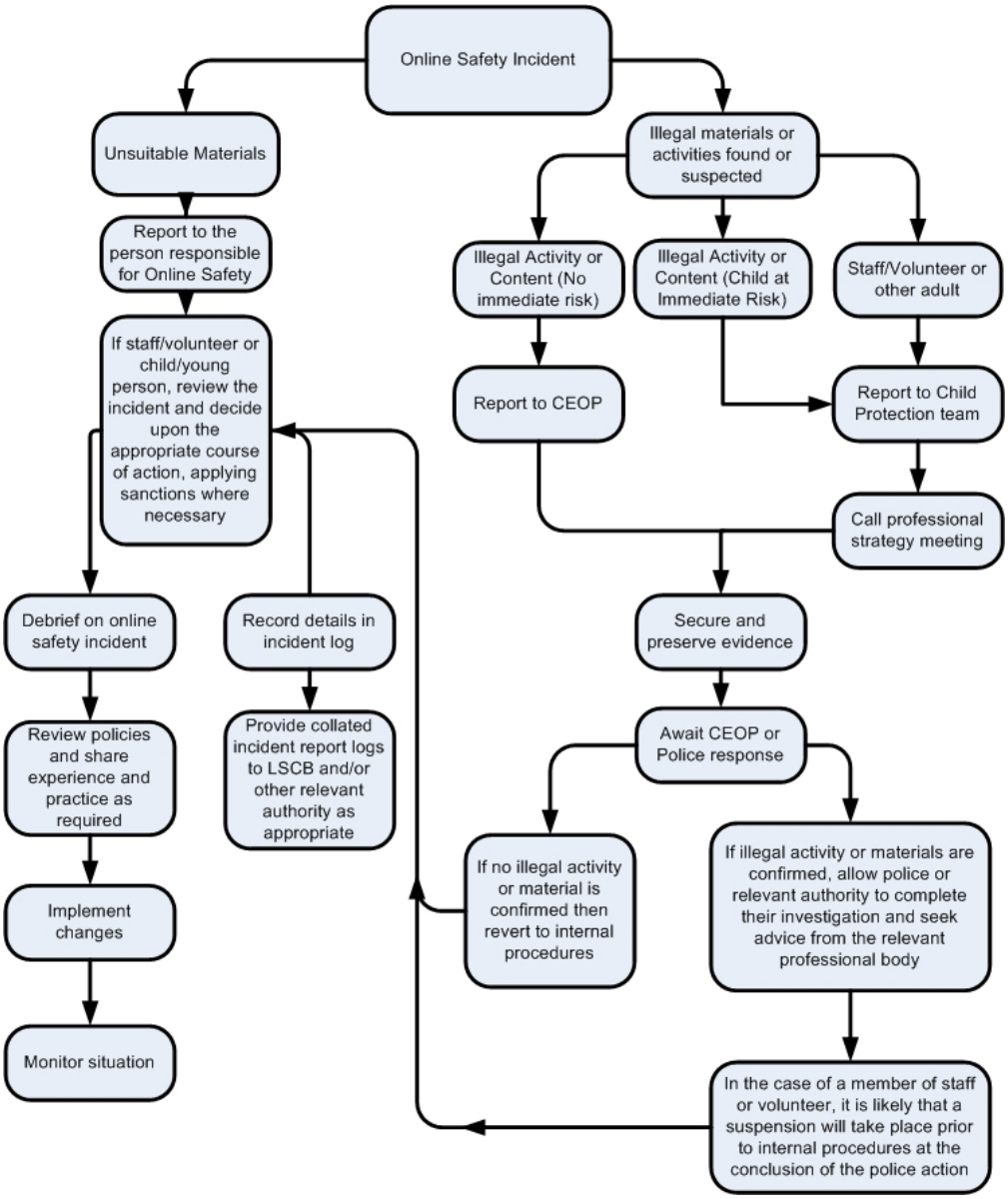
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce e.g. break times, Young Enterprise			X			
Illegal file sharing					X	
Use of social media in a professional capacity				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube				X		

Responding to incidents of misuse

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 (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the website(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 (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will 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.

In the event of suspicion, all steps in this procedure should be followed:

- **If content being reviewed includes images of child abuse, 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**
- **Disable user accounts if necessary**
- Have more than one member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise.
- It is important to ensure that the relevant staff should have appropriate internet access (e.g. social networking) to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also 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 form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated, the E-Safety Coordinator 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 by Local Authority or national / local organisation (as relevant)
  - Police involvement and/or action

It is important that all of 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 should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

It is more likely that the school 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 members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students

Referrals / Actions / Sanctions available

Incidents: In more serious circumstances we reserve the right to apply any of the sanctions available	Refer to class teacher / tutor	Refer to Head of Year / Learning Manager	Refer to technical support staff for action re filtering / security etc	Refer to Headteacher	Refer to Police	Warning	Inform Parents / Carer	Removal of network / internet access rights	Further sanction e.g. detention / internal exclusion / exclusion internal exclusion
	Referrals					**Actions**		**Sanctions**	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X		X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X			X	X		
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X	X		
Unauthorised use of social media / messaging apps / personal email	X	X	X			X	X		
Unauthorised downloading or uploading of files	X	X	X			X	X		
Allowing others to access school network by sharing username and passwords		X	X			X	X		
Attempting to access or accessing the school network, using another student's account		X	X			X	X		
Attempting to access or accessing the school network, using the account of a member of staff		X	X			X	X		
Corrupting or destroying the data of other users		X	X			X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X		
Using offensive and inappropriate language		X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X		X	X	X	X
Continued infringements of any of the above, following previous warnings or sanctions		X	X	X		X	X	X	X

Staff

Referrals / Actions / Sanctions available

Incidents: In more serious circumstances, we reserve the right to apply any of the sanctions available	Refer to line manager	Refer to Technical Support Staff for action re filtering etc	Refer to Headteacher	Refer to Local Authority	Refer to Police	Warning	Removal of network / internet / social networking access rights / computer ICT equipment	Disciplinary Action	Suspension
	Referrals					**Actions**		**Sanctions**	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X		X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X			
Unauthorised downloading or uploading of files	X	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				X			
Careless use of personal data e.g. holding or transferring data in an insecure manner	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 or of a bullying nature	X		X			X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with Students	X		X			X		X	X
Actions which could compromise the staff member's professional standing	X		X			X			
Actions which could bring the school 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			X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X			
Breaching copyright or licensing regulations	X					X			
Continued infringements of the above, following previous warnings or sanctions	X		X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X		X	X
Deliberate actions to breach data protection or network security rules	X	X	X			X		X	X

Appendix A - Student ICT Acceptable Use Policy

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital 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.

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

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices, internet, email and other 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 online and I know that people online may not be who they seem.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report to a member of staff any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will not visit unsafe sites or register for things I'm not old enough for. I understand this could put me at risk.
- I understand that different sites have safety features and use them.
- I will take care about what I publish on the web as I know once published I cannot control what it is used for.
- I will make sure my teacher / parents know who I communicate with online.
- I will log off sites and computers when finished.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the school systems or devices for online gaming, online gambling, online buying or selling, internet shopping and illegal file sharing.
- I will not use video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other users' files, without the owners' knowledge and permission.
- 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 will only use my own personal devices (mobile phones / tablet / USB devices / camera etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement and in the school mobile device policy, in the same way as if I was using school equipment.
- 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 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 damage or faults involving equipment or software, irrespective of how 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 device settings.
- I will only use social media sites that the school allows, with permission and at the times that are allowed.

When using the internet for research, I recognise that:

- I should 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 try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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 and the school e-safety policy, 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 will be subject to disciplinary action as outlined in the school e-safety policy. This may include loss of access to the network, internet, detentions, sanctions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

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)
- I use my own devices in the school (when allowed) e.g. mobile phones, tablets, USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Parent / Carer Countersignature

- As the parent / Carer of the below student, I give permission for my son / daughter to have access to the network, internet, Google Apps for Education, Office 365 and to the necessary associated ICT systems at Idsall School.
- 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 e-safety.
- As parent / carer I am aware of the importance of e-safety and I encourage the education and guidance of young people with regard to their on-line behaviour. I will support the school in enforcing this acceptable use policy.

Appendix C - Staff and Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This ICT Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT 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 ICT in their everyday work.
- that staff can guide students in good e-safety practice to keep them safe online.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff to agree to be responsible users.

ICT Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications. Automated software scans all email for viruses, spyware and offensive content.
- I understand that the rules set out in this agreement also apply to use of all school ICT systems (e.g. school devices, email, cloud systems, SIMS) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use. If I use the systems for personal or recreational use, I understand that excessive personal use is not acceptable, and I may be asked to remove excessive amounts of personal pictures, videos and music including personal iTunes accounts.
- I will not disclose my password to anyone else (unless requested by IT Support), nor will I try to use any other person's username and password (this excludes IT Support). I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will ensure passwords meet basic complexity. ICT Systems will enforce staff passwords are changed every 120 days, are at least 8 characters long, contain a capital letter, contain a number or symbol and are not allowed to use any of the last 3 passwords. To enhance account security, Microsoft Office 365 accounts will require Multi Factor Authentication via a call / text / email when accessed by staff and trustees off the school premises.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Deputy Head (Ms D Campbell).

I will be professional in my communications and actions when using *school* 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 which is contained within the school e-safety policy. I will not use my personal equipment to record these images, unless I have permission to do so and then in accordance with the school's policy on the use of digital / video images. Where these images are published (e.g. on the school website / social networking / VLE) it will not be possible to identify by full name, or other personal information, those who are featured. Students should not be identifiable by surname.
- I will only use chat and social networking sites that the school approves. Staff that require access to social networking sites for official school use should read and sign the additional social networking access form which is available on request from IT Support.
- I will only communicate with students and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- For further email advice please refer to separate email guidance.

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

- When I use my own personal mobile devices (tablet / laptops / 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 set by the school about such use contained in the school e-safety policy. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- Although the school permits access to personal email / cloud accounts, staff are not permitted to communicate with students, parents, Trustees or contractors via these systems. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications). Staff should also not transfer school data via these personal email / cloud systems.
- When I leave my computer unattended I will 'lock' (+ L) the computer to stop other unauthorised individuals gaining access to it.
- 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 (due to the risk of the attachment containing viruses or other harmful programmes).
- 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 only install programmes on a computer that are correctly licensed. The school is not licensed for software purchased by individuals for home use.
- I will not disable or cause any damage to school equipment or 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. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student 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 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).

Idsall School Network Access
Application for Account

I wish to apply / reapply (*delete as appropriate*) for an Idsall School Network account and user name. I wish to have an email account, be connected to the intranet and internet, and be able to use the school's ICT resources and systems.

I confirm that I have been given a copy of the Idsall School Staff AUP.

I confirm that I am aware that a copy of the Idsall School E-Safety Policy is available at:
S:\Staff files\Policies\ICT Security Policies\E-Safety-Policy.docx

I confirm that I have been given a copy of the Idsall School E-Mail Guidance.

I understand that these rules are in place to enable me to use ICT safely and if I fail to comply with this ICT Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension or a referral to Trustees and in the event of illegal activities the involvement of the police. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home
- I use my own ICT (when allowed) in school
- I use my own ICT out of school to use school sites or for activities relating to my employment by the school

I do / do not require SIMS (school database) access (*delete as appropriate*)

User's Full Name _____ please print

Job Title _____

User Signature _____ Date _____

Start Date _____ Leaving Date If Temporary _____

For IT Support Use:

Continuation Account ☐ New Account ☐

Network account setup by ……... Setup Date ……
Username……

Logon Tested ☐ Sims Account Set Up ☐ Sims Password Emailed ☐

Show My Homework Account ☐ Parents Evening System Account ☐

Other Notes
……

Laptop / Device Loan Agreement

The school provides teaching staff and some support staff with a loan of a laptop and/or iPad to carry out their duties. This document is an agreement between both staff and school and shall be binding for the duration of the device loan.

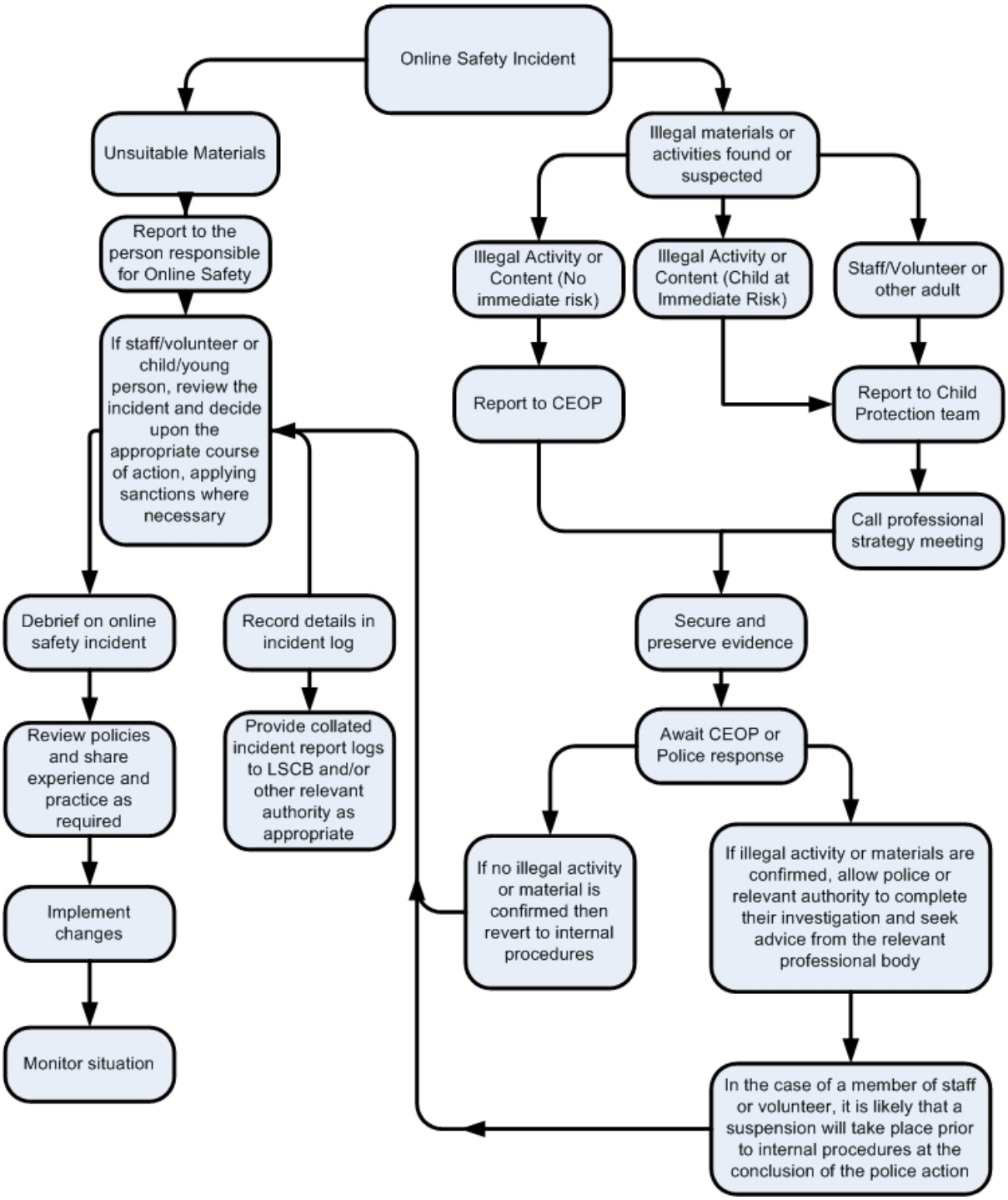
- The device shall remain the property of the school for the duration of the loan.
- The device shall be retained by staff in order to exercise their professional duties.
- The device shall be returned to school upon a member of staff terminating their employment with the school and any additional software/saved data removed.
- The device shall be available for use in school each day.
- Staff will be expected to use the device to assist in their professional duties.
- Staff are to take proper care of the device at all times.
- School devices should not be decorated or personalised in any way due to the fact that they may be reallocated to other members of staff.
- Staff shall be responsible for the security of the device ensuring it is in a locked cupboard/office when unattended in school and ensuring all reasonable precautions are taken when transporting the device, devices are uninsured by the school when left in cars. A Kensington lock can be provided on request.
- Software installed on the devices is to be correctly licensed, you must not install any unlicensed software.
- If your device is recalled by ICT Support for service/upgrade, you must bring it when specified.
- Staff should not interfere with the encryption, windows update and anti-virus systems installed on devices.
- Although we provide systems to back up data on your laptop, it is your responsibility to ensure that any work saved on the laptop is backed up onto your N: Drive on a regular basis to avoid loss of data. It is also recommended that you make your own backups of data.
- All faults are to be reported to ICT Support as soon as possible. (Ext 417).
- If a virus warning is received, you must report it to ICT support immediately. You will hand over your laptop immediately if ICT Support deem it necessary.

I _____agree to the terms and conditions above

Signed _____ Date_____/_____/_____

Laptop/iPad Name (see IT Support if unsure) (see example below)	Serial No (see IT Support if unsure) (see example below)	I am in possession of this device - Staff Signature	Returned on date and ICT Support Staff Signature (**office use only)**
TOSH??????	4E115037S	Sign	
iPad-??	DMPK6K2TF182	Sign	

Appendix E - Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

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 websites)

Website(s) address / device	Reason for concern

Conclusion and action proposed or taken

Appendix F - Template Reporting Log

Reporting Log Group	Date	Time	Incident	Action taken		Incident Reported by	Signature
				What?	By whom		

Appendix G - School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Network Manager.

Technical Security

Policy statements

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

- **School 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**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff**
- **All users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Network Manager 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.
- *Mobile device security and management procedures are in place.*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*

- *Remote management tools (Impero) are used by staff to control workstations and view users activity.*
- *An appropriate system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator / Network Manager / Technician.*
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.*
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy in the appendix for further detail).
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy in the appendix for further detail).

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed.
- *Passwords for new users, and replacement passwords for existing users will be allocated by IT Support*.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Users will change their passwords at regular intervals – as described in the staff and student sections below*.
- The level of security required may vary for staff and student accounts and the sensitive nature of any data accessed through that account.
- *Requests for password changes should be authenticated by IT Support to ensure that the new password can only be passed to the genuine user.*

Staff passwords:

- **All staff users will be provided with a username and password** by *IT Support who will keep an up to date record of users and their usernames in Active Directory*
- *The password should be a minimum of 8 characters long and must include three of – upper case character, lower case character, number, special characters*
- To enhance account security, Microsoft Office 365 accounts will require Multi Factor Authentication via a call / text / email when accessed by staff and trustees off the school premises
- *Must not include proper names or any other personal information about the user that might be known by others*
- *The account should be "locked out" following six successive incorrect log-on attempts*
- *Temporary passwords e.g. Used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *Passwords shall not be displayed on screen*
- Should be changed at least every 120 days
- Should be significantly different from previous password *the last three passwords cannot be re-used* passwords created by the same user
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- Should be different for systems used inside and outside of school

Student / pupil passwords

- **All users will be provided with a username and password** by *IT Support who will keep an up to date record of users and their user names in Active Directory*
- *Users will be required to change their password every 120 days*
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (Network Manager) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User log-ons*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so as the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be logged in change control logs**
- **be in liaison with a second responsible person**

All users have a responsibility to report immediately to Network Manager any infringements of the school's filtering policy of which they become aware, or any sites that are accessed which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider (Sophos / Wave9 Managed Internet Services Ltd) by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *The school maintains and supports the managed filtering service provided by the Internet Service Provider* (Sophos / Wave9 Managed Internet Services Ltd)
- *The school has provided enhanced / differentiated user-level filtering through the use of the* Sophos *filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader)*
- *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical.If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group*

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *the Acceptable Use Agreement*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement (AUP) and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will, therefore, monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement (AUP). *Monitoring will take place as follows:*

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *E-Safety Coordinator / E-Safety Group E-Safety Trustee / Trustees committee / External Filtering provider / Local Authority / Police on request*

Appendix K – Electronic Devices - Searching & Deletion

POLICY DOCUMENT	**Electronic Devices - Searching & Deletion**
STATUTORY FOR ACADEMY SCHOOLS	
Legislation: Education/Other	
Lead Member of Staff	D. Campbell – Deputy Headteacher
Lead Trustees (monitoring)	
Publication /Revision Date	January 2023
Governor Committee	Behaviour and Safety Committee
Committee Approval Date	Reviewed by e-safety committee January 2023
Full Trustees Ratification Date	
Review Frequency	Annually
Date of next review	January 2024
Publication date: **School Website** **Staff Information folder**	October 2015
Chair of Governing Body signature	
Purpose	To ensure that the Headteacher and The Governing Board act in accordance with the law on data protection
Supporting documents	e-Safety policy

School Policy: Electronic Devices - Searching and Deletion

Introduction

The changing face of information technologies and ever-increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will, however, help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item may only be searched for under these new powers if it has been identified in the school rules as an item that is believed to have **been used to carry out an action banned by the school rules.** It is, therefore, important that there is a school policy which sets out clearly and unambiguously the items and/or actions which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should, therefore, be clear links between this policy and the behaviour policy).

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Trustees for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by the Deputy Head responsible for e-Safety and will be reviewed by the Trustees.

The Headteacher has authorised (subject to training) the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

- All Heads of Year
- KS3 Manager
- KS4 Manager
- All SLT members
- Child Protection Officers

The Headteacher must authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

NOTE: Members of staff cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's e-safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. (see e-Safety Policy).

If pupils / students breach these rules:

The sanctions for breaking these rules can be found in the e-Safety Policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - authorised staff may search with the pupil's consent for any item.
- Searching without consent - authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

(NOTE: Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the *student* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student* being searched.

There is a limited exception to this rule: authorised staff can carry out a search of a *student* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the *student* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the *student* has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the *student* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. *(NOTE: It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.)*

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

Members of staff may require support in judging whether the material is inappropriate or illegal. The Child Protection Officers should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school will also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so *(i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).*

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. *(NOTE: It is recommended that members of staff should contact a Child Protection Officer, within school, for further guidance before taking action and that the person or persons is or are named within this policy).*

A record should be kept of the reasons for the deletion of data / files.

(DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

Audit / Monitoring / Reporting / Review

The responsible person, (Senior Leader with responsibility for the Pastoral System) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by *E-Safety Officer / E-Safety Committee / E-Safety Trustee* at regular intervals when the e-Safety Committee meets.

This policy will be reviewed by the Headteacher and Trustees annually and in response to changes in guidance and evidence gained from the records.

DfE advice on these sections of the Education Act 2011 can be found in the document:
"Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Appendix L – Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) works very simply. Students connect to the **school** BYOD wi-fi signal by entering their usual school network credentials and then once again enter their network credentials into a portal after which they will have access to the internet. This facility will be securely filtered and subject to the standard Acceptable Use Agreement. Access is only available to 6th form students who have completed a Student Acceptable Use Agreement.

General information

Access to the wireless facility is filtered in compliance with the school Acceptable Use Policy. Access from personal devices is limited to internet use only. Users will not have direct access to any documents or facilities that reside on the school network from their personal devices except for access via iSchool and windows desktop remote access. Access to the wireless facility is a privilege, not a right. Any use of the facility entails personal responsibility and compliance with all the school's rules and policies. Gaming devices are NOT allowed.

Guidelines for use

- Use of personal devices during the school day is at the discretion of staff.
- The primary purpose of the use of personal devices at the school is educational.
- The use of a personal device is not to be a distraction in any way to staff or other students.
- The Idsall School ICT Acceptable Use Agreement applies to the use of personal devices.
- Students must bring their personal devices to school fully charged and are **NOT** permitted to recharge their devices on school property unless an electrical test certificate is provided, or alternative arrangements as agreed with the school.
- Students must not attempt to circumvent the school network security and/or filtering. This includes attempting to bypass proxies.
- Devices must be in silent mode at all times.

Consequences for misuse/disruption (one or more may apply)

- The device may be confiscated for the period or rest of the day
- The device may be confiscated until a parent/carer collects it
- The student may be refused permission to use personal devices on school property
- Disciplinary action may be taken in accordance with existing school policies

School liability statement

Users bring their own personal device(s) to use at Idsall School at their own risk. It is your duty to be responsible in the up-keep and protection of your device(s). Access to the facility may be monitored, suspended or terminated at any time if this agreement is not adhered to.

Idsall School will **NOT** be responsible for:

- Personal devices that are broken or damaged while at school or during school-related activities
- Personal devices that are lost or stolen at school or during school-related activities
- Maintenance or upkeep of any personal devices
- Technical support of personal devices

Appendix M - Social network accounts by staff for use in education

When a school leader or member of staff wishes to create a social networking site profile/page for use in a professional capacity (e.g. a school Facebook page, a blog about a school event, a class twitter account) the following guidelines must be followed:

- All social media services must be approved by the SIRO or Headteacher in advance of any work being undertaken.
- Passwords should be complex (i.e. 8 or more characters including uppercase, lowercase, numbers and symbols) and changed regularly.
- Administrator email addresses should be email accounts provided by the school and not personal email accounts.
- Social media services must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages.
- Social media services must not be used for the promotion of personal financial interest, commercial ventures or personal campaigns.
- Social media services must not be used for actions that would put school staff in breach of school codes of conduct or policies.
- Staff should not use the account to enter into direct communication with pupils that would breach the guidance in the Staff ICT Acceptable Use Policy.
- The social media site should be used purely for educational purposes and not personal purposes.
- Photos/videos of pupils should not be posted unless permission has been gained from parents/carers.
- Surnames of pupils should never be published.
- Do not directly refer to or link to any individual's social networking profile.

I agree to follow the above guidelines in the creation of social network accounts by staff for use in education.

Name _____

Position _____

Signed _____

Date _____ **Approved by E-Safety Coordinator** _____

Appendix N - Staff Email Policy

Idsall School is committed to providing Internet and e-mail facilities to employees where an educational need is established and to promote employee awareness of the benefits and potential dangers involved. Email is also an important school communication system. This guidance sets out guidelines for employee use. The school email is provided by Idsall School and is governed by the Acceptable Use Policy.

Email Policy

- As an authorised user of an Idsall School email address, I understand that this email address must be used for all professional communication.
- I will use alternate email addresses for private communications.
- I understand that the email system is monitored and should not be considered private communication. Automated software scans all email that could compromise the integrity of the computer systems or contain viral/unsuitable/offensive content.
- I will not email school data to personal email addresses as this may compromise data protection.
- If I have a need to email school data to any 3rd party e.g. (IAmLearning/Kerboodle) then this data must be encrypted. IT Support can advise on how to do this.
- As a user of the email system, I recognise that teaching and learning is the primary role of staff and understand staff cannot be expected to respond immediately to email when they are teaching.
- I will, when possible during a typical working day, check my emails daily.
- If possible, reply within 48 hours as ignoring messages is discourteous and confusing to a sender.
- I understand that pupils are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use.
- I understand that all emails sent and received are considered the responsibility of the user.
- I will use student distribution lists (SDL) as appropriate to limit blanket emails, for example, I could email all teachers of Joe Bloggs by sending it to 'SDL Joe Bloggs'.
- If you receive an inappropriate email, it should be reported to the appropriate person depending on the nature of the email e.g. Line Manager, IT Network Manager, E-Safety Coordinator or Headteacher.
- Clearly identify the topic in the subject field.
- A message should be about a single topic. If you want to raise a second topic, send another message to avoid having content unrelated to the message heading.
- Change the subject line if the topic changes in your reply.
- DO NOT USE ALL CAPITALS, AS IT MAY BE INTERPRETED AS SHOUTING!

- When replying to a message that has been sent to a list of recipients, only reply to the whole list if your answer is of interest to them all! If you are taking up specific points with the sender of the original message, send your response only to that person.

- All emails sent must remain at a professional level.

- Staff should not distribute large documents as attachments to multiple users (e.g. distribution groups – curriculum staff, support staff and school admin) – these documents can be placed on the school network and shared via a hyperlink. IT Support can give advice on how to use a hyperlink.

- Consider carefully to whom any email is cc'd. Try to avoid staff receiving excessive amounts of messages in their inboxes. The staff intranet/VLE, staff briefing, and student bulletin can be used for general announcements.

- The mail server supporting the email system is not intended for the long-term storage of messages. Housekeeping of stored messages is your responsibility. When you receive an email message with an attachment, save the attachment to your user area. From time to time, you should delete unwanted sent, deleted and received emails.

- Do not reply to 'junk or spam' email, this indicates to the sender that your email account is 'live'. The best way to deal with 'junk or spam' email is to delete it, do not forward it on to anyone else. The school does have anti-spam email systems but unfortunately some spam does still slip through.

- Please be aware that email communications can be presented as evidence in court of law and are legally binding.

- Do not open attachments from senders you do not recognise, or that look suspicious, just delete it, do not forward it.

- Do not use deleted items as a storage area. Deleted items should be permanently deleted regularly.

Appendix H
Idsall School
Backup Strategy

Policy Context

The backup solution at Idsall School is based on a Microsoft Data Protection Manager 2016 (DPM). It provides a combination of local Disk to Disk backup (D2D) which enables quick recovery and Disk to Microsoft Azure Cloud backup (D2C) which gives us long term offsite backup. All backups are encrypted.

1. All administrative and financial data is backed up daily. Backup is first taken via local disk to disk (D2D) and stored on a Network Access Storage (NAS) storage device stored securely in the Skills Centre away from the main school building. This local backup is stored for 84 days.

2. All curriculum data is backed up daily. Backup is firstly taken via local disk to disk (D2D) and stored on a Network Access Storage (NAS) storage device stored securely in the Skills Centre away from the main school building. This local backup is stored for 84 days.

3. Other critical data is backed up daily. Backup is firstly taken via local disk to disk (D2D) and stored on a Network Access Storage (NAS) device stored securely in the Skills Centre away from the main school building. This local backup is stored for 84 days.

4. Other non-critical data is backed up daily. Backup is firstly taken via local disk to disk (D2D) and stored on a Network Access Storage (NAS) device stored securely in the Skills Centre away from the main school building. This local backup is stored for 28 days.

5. Backups are also taken to Microsoft Azure Cloud for offsite protection. Backup to Cloud (D2C) of each server will take place weekly.

6. Backups should be checked regularly to ensure that they have been successful. For example, if a backup has been made to a cloud, the contents should be checked to see that a file, or files exist, and that their date of creation is consistent with the date of the backup.

Below is a list of servers, data and backup restore points.

Server	Data	Disk Backups in days	Cloud backup in weeks
WIN2K12ADM	SIMS	64	12
WIN2K8ADM	FINANCE DATA	64	12
WIN2K19STA	STAFF SHARED (S:)	64	12
HYPER-V	WIN2K16DC VM Network	30	4
HYPER-V	WIN2K12NT VM	30	0
HYPER-V	WIN2K8SCCM VM	30	0
IMPERO	IMPERO & SPICEWORKS	30	0
DPM	DPM DATABASE	30	12
VARIOUS	SYSTEM STATE	30	12

Appendix P – Access to systems by contractors

This agreement should be signed by all contractors accessing school systems or facilities prior to access being granted.

By signing this form, you are agreeing:

- to comply with the school's Information Security Policy and procedures and take all necessary steps to ensure the security integrity and confidentiality of all data and other information held by the school to which you shall have access
- to conform with the provisions of all relevant legislation inclusive of but not limited to the Data Protection **Act 1998, Copyright Designs and Patents Act 1988, Computer Misuse Act 1990 and** all subsequent relevant legislation
- that you will not, wit**h**out the prior consent of the school in writing, divulge data or any other information provided to you by the school or held by the school to which you shall have access
- that you will take all reasonable precautions to ensure that viruses or other malicious software are not introduced onto or into the school's IT facilities or systems
- that you will not without the previous consent of the school in writing make any change or alteration to IT facilities or systems used by the school
- that you will not access any of the school data information systems or facilities unless it is required to do so under the terms of the Contract and in any event not without the school's prior consent in writing. This includes only accessing information or systems specified by the school and in accordance with agreed times of access
- will not disclose methods of access to facilities or systems to any person without the school's prior consent in writing
- will not download the school's accessed data or other information without the school's prior consent in writing

The Contractor shall fully indemnify Idsall School against all damages (excluding consequential damages), costs, charges and expenses arising from or incurred by its failure to comply with the above clauses and shall promptly notify Idsall School in writing of any alleged infringement of which the Contractor has notice of. The Contractor will make no admissions of liability without Idsall School's prior written consent. The provisions of this Clause shall survive the expiration or termination of this or any related Agreement.

Please sign below to acknowledge that you have read and understood this document and agree to the conditions therein.

Signed: _____Name: _____

Date: _____Organisation: _____

Appendix Q – Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

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

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent; there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012
Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Appendix R - Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

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/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

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

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

E-Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the [school/ academy] community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-safety committee will seek to include representation from all stakeholders.
The composition of the group should include:

- SLT member/s
- Child protection/safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator
- Trustee
- Parent / Carer
- ICT Technical Support staff
- Student representation

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:
- Staff meetings
- Student forums (for advice and feedback)
- Trustees meetings
- Surveys/questionnaires for students, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for Idsall School have been agreed.

Signed by (SLT):

Date:

Date for review:

Acknowledgement

Appendix T - Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
BYOD	Bring Your Own Device
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

APPENDIX U PREVENT Strategy

Preventing Radicalisation and Extremism

The school's **Child protection policy** which is available on our website (www.idsallschool.org) and in school, covers Radicalisation and Extremism.

CONTEXT: The internet, in particular social media, is being used as a channel to promote and engage. Often this promotion glorifies violence, attracting and influencing many people including children and in the extreme cases, radicalising them. Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it.

This threat is not just from groups, such as Islamic State, but from 'far right' groups also.

Indicators of Vulnerability to Extremism and Radicalisation

1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2. Extremism is defined by the Government in the Prevent Strategy as:
   Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

3. Extremism is defined by the Crown Prosecution Service as:
   The demonstration of unacceptable behaviour by using any means or medium to express views which:

   - Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
   - Seek to provoke others to terrorist acts.
   - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
   - Foster hatred, which might lead to inter-community violence in the UK.

4. There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5. Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

6. Indicators of vulnerability include:

   - Identity Crisis – the student / pupil is distanced from their cultural / religious heritage and experiences discomfort about their place in society.

- Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
- Personal Circumstances – migration; local community tensions; and events affecting the student / pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
- Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
- Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration.
- Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

7. However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

8. More critical risk factors could include:

- Being in contact with extremist recruiters.
- Accessing violent extremist websites, especially those with a social networking element.
- Possessing or accessing violent extremist literature.
- Using extremist narratives and a global ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Joining or seeking to join extremist organisations.
- Significant changes to appearance and / or behaviour.
- Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

Preventing Violent Extremism

Roles and Responsibilities of the Point of Contact (POC); the POCs for Idsall School are Cath Cork (Assistant Headteacher) and Jennie Reeve (Pastoral Lead), who are responsible for:

- Ensuring that staff of the school are aware that you are the Point of Contact in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism; and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.

- Raising awareness about the role and responsibilities of Idsall School in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Monitoring the effect in practice of the school's RE curriculum (through liaison with the Head of RE, Mrs Calvert) and assembly policy (through liaison with Casey Bailey, Assistant Head) to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

- Liaising with the Idsall School network manager to ensure that appropriate levels of filtering and monitoring are in place to meet the needs of the school's Safeguarding and Child Protection policies and to meet the needs of the Prevent Strategy.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.

- Collating relevant information from in relation to referrals of vulnerable students / pupils into the Channel* process.

- Attending Channel* meetings as necessary and carrying out any actions as agreed.

- Reporting progress on actions to the Channel* Co-ordinator.

- Sharing any relevant additional information in a timely manner.

Channel is a multi-agency approach to provide support to individuals who are at risk of being drawn into terrorist related activity. It is led by the West Midlands Police Counter-Terrorism Unit, and it aims to

- Establish an effective multi-agency referral and intervention process to identify vulnerable individuals.
- Safeguard individuals who might be vulnerable to being radicalised, so that

they are not at risk of being drawn into terrorist-related activity; and

- Provide early intervention to protect and divert people away from the risks they face and reduce vulnerability.

- For more information on PREVENT please follow this link: https://www.gov.uk/government/policies/protecting-the-uk-against-terrorism/supporting- pages/prevent
- For more information about the Home Office's radicalisation awareness training product Workshop to Raise Awareness of Prevent (WRAP) email: WRAP@homeoffice.x.gsi.gov.uk
- If you have a concern about a child in respect of extremism, please report them to Cath Cork (Assistant Headteacher) and Jennie Reeve (Pastoral Lead). Additional support is available from the LSCB police representative who will be able to discuss support options.
- To report suspected online terrorist content, please follow this link https://www.gov.uk/report-terrorism
- You can also refer content of concern directly to social media platforms - find out how: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

SWGfL / UK Safer Internet Centre

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety in addition to its commitment to provide educational establishments in the South West of England with safe, secure and reliable broadband internet connections and broadband-enabled teaching & learning resources and services.

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk/

SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa. More information about its wide-ranging e-safety services for schools can be found on the SWGfL website – www.swgfl.org.uk

360 degree safe E-Safety Self Review Tool

360 degree safe is an online, interactive Self Review Tool which allows schools to review their e-safety policy and practice. It is available, free of charge, to all schools - with over 4,000 registrations, since its introduction in 2009.

Schools choose one of 5 level statements in each of the 28 aspects. The tool provides an "improvement action" describing how the school might move from that level to the next. Users can immediately compare their levels to the benchmark levels of all the schools using the tool. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources / good practice guidance and collates the school's action plan for improvement. Sections of these policy templates can also be found in the links / resources section in 360 degree safe.

Schools that reach required benchmark levels can apply for assessment for the E-Safety Mark, involving a half day visit from an accredited assessor who validates the school's self-review. More information about the E-Safety Mark can be found at: http://www.360safe.org.uk/Accreditation/E-Safety-Award

SWGfL BOOST+ – Schools online safety toolkit

The SWGfL BOOST+ package brings you extra empowerment and support to deal with your online safety challenges, official or otherwise. It comprises a toolkit of apps, services, tools, CPD training and resources that all go to save time, equip your school to be more sensitive to, and better manage, online safety situations and issues. This document will reference specific aspects of BOOST to illustrate how it integrates with policy. For further information on BOOST+, please visit http://boost.swgfl.org.uk/home.aspx