eSafety Policy

Autumn 2021

eSafety 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 and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe Internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school eSafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put children at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other school policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The eSafety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Schedule for this Policy

This eSafety policy was approved by the Governing Body on:	June 2020
The implementation of this eSafety policy will be monitored by:	Saira Sawtell (SLT / Headteacher) Paul Absolom (SLT / Designated Safeguarding Lead & SENDCO), Gareth Biddle (SLT / Behaviour and Pupil Wellbeing) Lizzy Pike (Computing Lead) Emily White (Chair of Governors) Nikki Fowler (Governor responsible for Safeguarding) Rob Fitzgerald (Site Manager)
Monitoring will take place at regular intervals:	Autumn Term
The Governing Body will receive a report on the implementation of the eSafety policy generated by the monitoring group (which will include anonymous details of eSafety incidents) at regular intervals:	Termly in conjunction with safeguarding reports
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place. The next anticipated review date will be:	Autumn Term 2021
Should serious eSafety incidents take place, the following persons / agencies should be informed:	Dorset Local Authority IT Manager Dorset Local Authority Safeguarding Officer / LADO Police Commissioner's Office Saira Sawtell – Headteacher Paul Absolom – Designated Safeguarding Lead (DSL) Nikki Fowler – Governor responsible for Safeguarding

Scope of this Policy

This policy applies to all members of the St Osmund's CE Middle School (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other eSafety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities:

Governors

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

- Regular meetings with the eSafety Officer (DSL)
- Regular monitoring of eSafety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors meeting

Headteacher/SLT

- The Headteacher has a duty of care for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Officer (DSL).
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff.
- The Headteacher and SLT are responsible for ensuring that the eSafety Officer and other relevant staff receive suitable training to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
- The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the eSafety Officer.

eSafety Officer (DSL)

- Takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with Leader for Computing and school technical staff (Network Manager)
- Receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments,
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends and reports to relevant meeting of Governors
- Reports to the Senior Leadership Team
- The production / review / monitoring of the school e-safety policy / documents
- The production / review / monitoring of the school filtering policy

Network Technicians

The Network Technicians, Lead for Computing and Headteacher are 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 eSafety technical requirements and any Local Authority eSafety Policy and 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 filtering policy (SWGFL), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- That the use of the network / internet / Office 365 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / SLT / eSafety Officer for investigation/action/sanction
- That monitoring software are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of eSafety matters and of the current school eSafety and Safeguarding policy and practices
- They have read, understood and accepted the Staff Acceptable Use Policy / Agreement (AUP) located in the school office
- They report any suspected misuse or problem to the Headteacher/SLT/eSafety Officer (DSL) for investigation
- All digital communications with pupils / parents/carers should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the eSafety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection/Safeguarding DSL

Should be trained in eSafety 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

Pupils

Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy found in the Home School Link Book

- 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 eSafety practice when using digital technologies out of school and realise that the school's eSafety 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 parents' evenings, newsletters, letters, website / Office 365 and information about eSafety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good eSafety 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 / Office 365 / social media counts and on-line pupil records

They are also responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy in the front of the Home School link book every year

Policy Statements:

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in eSafety is therefore an essential part of the

school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience.

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

- A planned eSafety input should be provided as part of Computing (and supported in PSHE) and is regularly revisited within all year groups
- Input annually from the Safe Schools Community Team (SSCT) with specific age appropriate input for each year group
- Key eSafety messages should be reinforced as part of the programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement within the Home School Link Book 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit using Netsupport Software as instructed during annual Safeguarding Inset sessions.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination…) that would normally result in internet searches being blocked. In such a situation, staff can request a temporarily removal for those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site – reference to relevant websites through an eSafety section
- Weekly posting of the 'National Online Safety' guidelines on the school Facebook page
- Parents evenings (annual SSCT parental sessions)
- Reference to the SWGfL safe website (Golden Rules for parents)

Education & Training – Staff

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

- eSafety training and updates will be available to staff as part of school Safeguarding Inset. eSafety training needs of all staff will be monitored regularly.
- All new staff should receive eSafety training as part of their Safeguarding induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Agreements.
- The eSafety Officer (DSL) will receive regular updates through reviewing guidance documents released by relevant organisations.
- This eSafety policy and its updates will be presented to staff within Safeguarding Inset.

- The eSafety Officer (DSL) will provide advice and organise for relevant training to individuals as required.

Education & Training – Governors

Governors should take part in eSafety training sessions as part of Safeguarding, with particular importance for those involved in technology / eSafety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority Governor Services or other relevant organisation.
- Participation in school training sessions for staff, governors or parents

Technical – infrastructure/equipment, filtering & monitoring

The school will be responsible for ensuring that the school infrastructure and 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 eSafety 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 technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- All users will be provided with a school email and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Dave Hewins – Network Manager, is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses 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.
- School network 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.
- An appropriate system is in place for users to report any actual / potential technical incident or security breach to the relevant person.
- 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.

Digital and video images – photographic & video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 but with direct permission from the Headteacher staff can use personal equipment for educational purposes only.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

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.
- 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 or any other removable media:

- The data should be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices eg tablets,	X						X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails		X						X
Use of messaging apps			X					X
Use of social media			X					X
Use of blogs			X					X

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

- The official school email service (365) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the DSL or a Deputy DSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, Office 365 etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use.
- Pupils should be taught about eSafety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on school website and only official email addresses should be used to identify members of staff.

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 (eg 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			

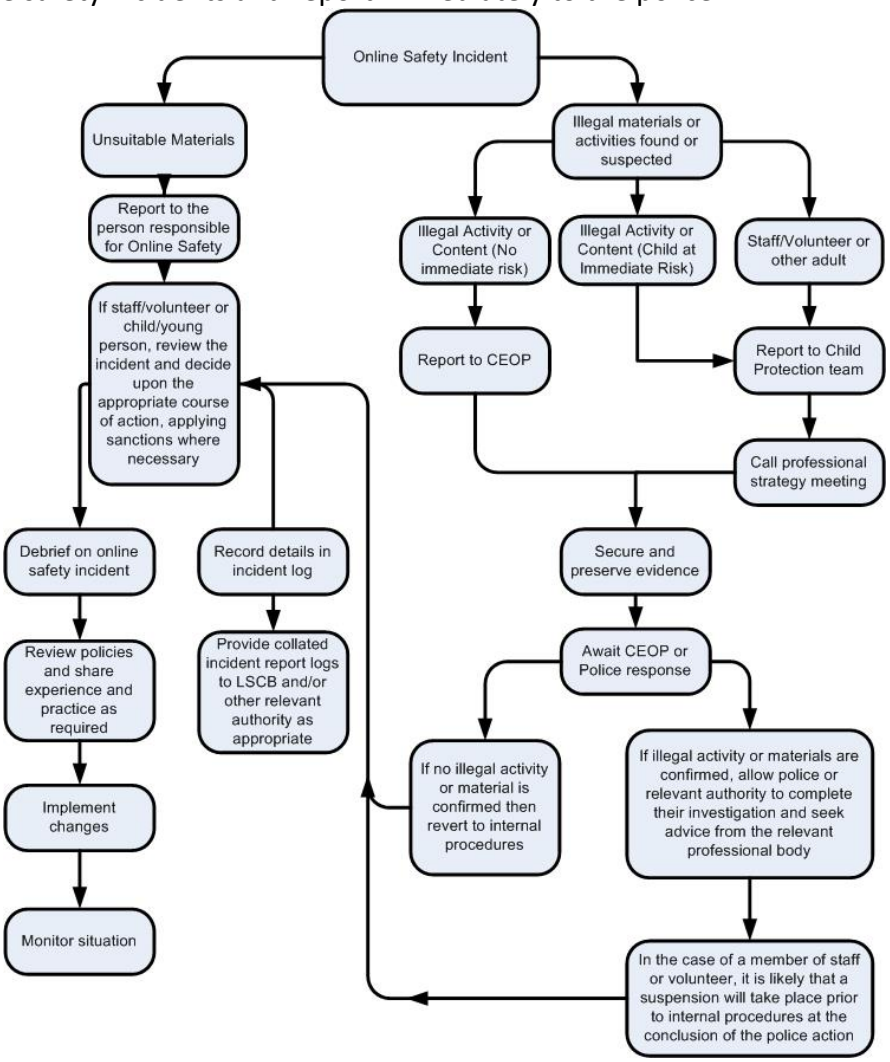
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing				X	
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

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 web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (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:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access 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 group 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

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the academy 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 & Sanctions

It is more likely that the academy 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:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Curriculum Lead / Year Lead or other	Refer to Headteacher / DSL	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents/carers	Removal of network / internet	Warning	Further sanction eg detention / exclusion
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
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	
Unauthorised use of social media / messaging apps / personal email	X	X						X	
Unauthorised downloading or uploading of files	X	X			X			X	
Allowing others to access school network by sharing username and passwords	X	X			X		X	X	X
Attempting to access or accessing the school network, using another pupil's account	X	X			X		X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	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	X	X	X
Continued infringements of the above, following previous warnings or sanctions	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	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			X	

Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		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	X	X	X

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X	X		X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	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	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X	X		X	X	X	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	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X		

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

Appendix

Privacy Notice

We are committed to safeguarding the privacy of our website visitors; this policy sets out how we will treat your personal information.

(1) What information do we collect?

We may collect, store and use the following kinds of personal data:

- Information about your computer and about your visits to and use of this website, such as your IP address, geographical location, browser type, referral source, length of visit and number of page views;
- Information that you provide to us for the purpose of registering with us;
- Information that you provide to us for the purpose of subscribing to our website services, email notifications and / or newsletters; and
- Any other information that you choose to send to us.

(2) Cookies

We use cookies on this website. A cookie is a text file sent by a web server to a web browser, and stored by the browser. The text file is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.

We may send a cookie which may be stored by your browser on your computer's hard drive. We may use the information we obtain from the cookie in the administration of this website, to improve the website's usability and for marketing purposes. We may also use that information to recognise your computer when you visit our website, and to personalise our website for you.

We may use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports about the use of the website. Google will store this information.
Google's privacy policy is available at: http://www.google.com/privacypolicy.html.

(3) Using your personal data
Personal data submitted on this website will be used for the purposes specified in this privacy policy or in relevant parts of the website.

We may use your personal information to:

- Administer the website;
- Improve your browsing experience by personalising the website;
- Enable your use of the services available on the website;
- Send you general (non-marketing) commercial communications;
- Send you email notifications which you have specifically requested;
- Send to you our newsletter and other]marketing communications (relating to our business) which we think may be of interest to you by post or, where you have specifically agreed to this, by email or similar technology (you can inform us at any time if you no longer require marketing communications to be sent by emailing us at);
- Provide third parties with statistical information about our users - but this information will not be used to identify any individual user; and
- Deal with enquiries and complaints made by or about you relating to the website.

We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing.

(4) Other disclosures
In addition to the disclosures reasonably necessary for the purposes identified elsewhere in this privacy policy, we may disclose information about you:

- To the extent that we are required to do so by law;
- In connection with any legal proceedings or prospective legal proceedings;
- In order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk); and
- To the purchaser (or prospective purchaser) of any business or asset which we are (or are contemplating) selling.

Except as provided in this privacy policy, we will not provide your information to third parties.

(5) Security of your personal data
We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

We will store all the personal information you provide on our secure servers. All electronic transactions you make to or receive from us will be encrypted using SSL technology.

Of course, data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

You are responsible for keeping your password and user details confidential. We will not ask you for your password.

(6) Policy amendments
We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page regularly to ensure you are happy with any changes. We may also notify you of changes to our privacy policy by email.

(7) Your rights
You may instruct us to provide you with any personal information we hold about you. You may instruct us not to process your personal data for marketing purposes by email at any time. (In practice, you will usually either expressly agree in advance to our use of your personal data for marketing purposes, or we will provide you with an opportunity to opt-out of the use of your personal data for marketing purposes.)

(8) Third party websites
The website may contain links to other websites. We are not responsible for the privacy policies or practices of third party websites.

(9) Updating information
Please let us know if the personal information which we hold about you needs to be corrected or updated.

(10) Contact
If you have any questions about this privacy policy or our treatment of your personal data, please write to us by email – office@stosmunds.dorset.sch.uk or by post to St Osmunds's CE Middle School, Barnes Way, Dorchester, DT1 2DZ.

Data Protection Policy

Schools, Local Authorities (LAs), and the Department for Education (DfE), the Qualifications and Curriculum Authority (QCA), Ofsted and the Learning Skills Council (LSC) all process information on pupils in order to run the education system, and in doing so have to comply with the Data Protection Act 1998. This means that data held about pupils must only be used for specific purposes allowed by law.

The school holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care and to monitor and assess how well the school progress. This information includes contact details, National Curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information. From time to time schools are required to pass on some of this data to LAs, the DfE and to agencies, such as QCA, Ofsted and LSC that are prescribed by law.

The Local Authority uses information about pupils to carry out specific functions for which it is responsible, such as assessment of any special educational needs the pupil may have. Information is also used to derive statistics to aid decisions (for example) on the funding of schools, and to assess the performance of schools and set relevant targets. Statistics are used in such a way that individual pupils cannot be identified.

The Qualifications and Curriculum Authority uses information about pupils to administer the National Curriculum tests and assessments for Key Stages 1 to 3. Results of these are forwarded to the DfE in order to compile national and regional trends and patterns in levels of achievement. The QCA information to evaluate the effectiveness of the National Curriculum and the associated assessment arrangements, to help ensure that these are continually improved.

Ofsted uses information about progress and performance of pupils to support inspector's evaluation of schools, to assist schools with their self-evaluation processes, and as part of the Ofsted's assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual pupils.

The Learning and Skills Council uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the education service as a whole. The statistics

(including those based on information provided by the QCA) are used in such a way that individual pupils cannot be identified. On occasion information may be shared with other Government departments or agencies strictly for statistical or research purposes only.

The Department for Education uses information about pupils for statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DfE will feed back to LAs and schools information about their pupils for a variety of purposes including data checking exercises, self-evaluation analyses and information missing from a former school.

The DfE will provide Ofsted with pupil level data for use in school inspection. Where relevant, pupil information may also be shared with post 16 learning institutions to minimise administrative burden on application for a course and to aid the preparation of learning plans.

Pupil information may be matched with other data sources the Department holds to model and monitor pupils' educational progression; to provide comprehensive information to LAs and learning institutions to support their day to day business. The DfE may also use contact details from these sources to obtain samples for statistical surveys: such surveys may be carried out by research agencies working under for the Department and participation in such surveys is usually voluntary. The Department may also match data from these sources to data obtained from statistical surveys.

Pupil data may also be shared with other Government Departments and Agencies (including the Office for National Statistics) for statistical or research purposes only. In all such cases the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports measures or decisions relating to particular individuals or identifies individuals in any results. This data will be approved and controlled by the Department's Chief Statistician.

The DfE may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have legitimate need for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them, with parents exercising this right on their behalf if they are too young to do so themselves.

If your child wishes to access their personal data, or you wish to do so on their behalf, then please contact the relevant organisation in writing:

- the school at Barnes Way, Dorchester, DT1 2DZ
- Simon Cull (the first point of contact for Data Protection issues) at Strategic Services, The Education Directorate, Dorset County Council, County Hall, Dorchester, Dorset DT1 1XJ
- the QCA's Data Protection Officer at QCA, 83 Piccadilly, London W1J 8QA
- Ofsted's Data Protection Officer at Alexandra House, 33 Kingsway, London WCB 6SE;
- LSC's Data Protection Officer at Cheylesmore House, Quinton Road, Coventry, Warwickshire CV1 2WT;
- the DfE's Data Protection Officer at DfE, Caxton House, Tothill Street, London SW1H 9NA.

In order to fulfil their responsibilities under the Act the organisation may, before responding to this request, seek proof of the requestor's identity and any further information required to locate the information requested. Separately from the Data Protection Act, regulations provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. If you wish to exercise this right you should write to the school.

Social Networking Policy

Section 1: Introduction 1.1 Objectives
1.1.1 This document sets out our school policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools staff in many ways. This document aims to:

- Assist schools staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Reduce the incidence of positions of trust being abused or misused

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their Headteachers of the justification for any such action already taken or proposed. Headteachers will in turn seek advice from the School's HR team where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix A.

1.1.4 This policy has been agreed following consultation with the recognised trade unions and professional associations.

1.2 Scope
1.2.1 This document applies to all staff who work in St Osmund's CE Middle School as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors and volunteers.

1.2.2 It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in schools. Reference to pupils means all pupils at the school including those over the age of 18.

1.2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of the management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.

1.2.3 The local authority is not able to accept liability for any actions, claims, costs or expenses arising out of a decision not to follow this recommended policy and its guidance, where it is found that the governing body has been negligent or acted in an unfair or discriminatory manner in exercising its employment powers.

1.3 Status
1.3.1 This document does not replace or take priority over advice given by HR, safeguarding boards or the school's codes of conduct, dealing with allegations of abuse other policies issued around safeguarding or IT

issues (email, IT and data protection policies), but is intended to both supplement and complement any such documents. This guidance has been agreed with the trade unions.

1.4 Principles

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Staff in schools should work and be seen to work, in an open and transparent way.
- Staff in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice in Schools

2.1 What is social media?

2.1.1 For the purpose of this policy, social media is the term commonly used for websites, which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Bebo and MySpace are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

2.1.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

2.2 Overview and expectations

2.2.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students public in general and all those with whom they work in line with the schools code of conduct. Adults in contact with pupils should therefore understand and be aware, that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

2.2.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of schools staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

2.2.3 School staff should always maintain appropriate professional boundaries and avoid behaviour during their use of the internet and other communication technologies which might be misinterpreted by others. They should report and record any incident with this potential.

2.3 Safer online behaviour

2.3.1 Managing personal information effectively makes it far less likely that information will be misused.

2.3.2 In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

2.3.3 All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any

photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

2.3.4 Staff should never 'friend' a pupil at the school where they are working onto their social networking site.

2.3.5 Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

2.3.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.

2.3.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school or another school or Dorset Council could result in formal action being taken against them.

2.3.8 Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications

2.3.9 Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or Dorset Council into disrepute.

2.3.10 Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstance this could damage the reputation of the school, the profession or the local authority.

2.4 Protection of personal information

2.4.1 Staff should ensure that they do not use school IT equipment for personal use, e.g. camera or computers.

2.4.2 Staff should keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.

2.4.3 Staff should never share their work log-ins or passwords with other people.

2.4.4 Staff should not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used.

2.4.5 Staff should keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.

2.4.6 Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

2.5 Communication between pupils / schools staff

2.5.1 Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

2.5.2 This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

2.5.3 It is the expectation that the school should provide a work mobile and e-mail address for communication between staff and pupils. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.

2.5.4 Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

2.5.5 Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

2.5.6 Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

2.5.7 E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

2.6 Social contact

2.6.1 Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

2.6.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.

2.6.3 There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

2.7 Access to inappropriate images and internet usage

2.7.1 There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

2.7.2 Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

2.7.3 Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools and school staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

2.7.4 Where indecent images of children are found by staff, the police and Local Authority Designated Officer (LADO) should be immediately informed. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate the matter or evaluate the

material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

2.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should refer to the dealing with allegations of abuse against staff and volunteers policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

2.8 Cyberbullying

2.8.1 Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate and individual in the attempt to gain power and control over them.'

2.8.2 Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e- mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

2.8.4 Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process. Employees will also have access to the Dorset Council staff counsellor, subject to funding being agreed.

2.8.5 Staff are encouraged to report all incidents of cyberbullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Section 3: Review of policy

3.1.1 Due to the ever changing nature of Information and Communication technologies it is best practice that this policy be reviewed annually and if necessary more frequently in response to any significant new developments in the use of technologies, new threats to eSafety or incidents that have taken place.

Section 4: Appendices

Appendix A – Relevant legislation

Schools staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

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 - 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 & 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 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) and you arrange 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 any 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.

Acceptable Use Policy – Staff

Guidance for the acceptable use of IT Equipment at St Osmunds

School Laptop	
You may	You should not
Use them for school related work	Download or install any software
Use them for suitable personal work, e.g. letter writing, internet use	Allow children to use them whilst logged as a member of staff
Connect them to your home network (including your printer)	Store images of St Osmund's Middle School children
	Use your school email address for personal communications (e.g. Banking, Amazon etc)
Your personal mobile Phone	
You may	You should not
Bring them into school	Access the internet using our wifi
Use them for personal reasons whilst not responsible for children (e.g. in the staffroom, or outside away from children)	Use them to take photographs of any St Osmund's Middle School children (including on school trips, sports fixtures etc)
	Use them for personal reasons whilst responsible for children (e.g. in the classroom, on break duty)
	Use them to access school email (photos are often stored on the device when opening an email)
School iPad / iPod / Camera	
You may	You should not
Us them for school related work. e.g. Use them to take group photographs of St Osmund's Middle School children Use them in lessons to display an app in the IWB	Allow other family members unrestricted use (i.e. tell them the password) as they contain, or give access to confidential information (e.g. email and photos etc)
Choose and Install Apps for use within school e.g. Draw Pad, Skitch	Store large amounts of personal data, e.g. music and photographs
Connect to your home wireless network and choose and install apps for personal use CAVEAT: you must apply your professional judgement as to their suitability	
Access your school email	Access personal email accounts
Update the school twitter feeds with appropriately professional tweets and photographs – large group photos only	
General	
You may	You should not
Store photographs of St Osmund's Middle School children (past or present) in the Photos folder on the T-Drive (please add sub folders of your own)	Permanently store photographs of St Osmund's Middle School children (past of present) anywhere else

Use school resources for personal reasons (e.g. small, infrequent personal printing, infrequent phone calls)	Use school resources for regular personal use
Use your own personal equipment (e.g. camera) to photograph St Osmund's Middle School children, provided you use a school memory card	Use your school email address for personal communications (e.g. Banking, Amazon etc)
	Use school equipment to store personal data e.g. photographs, music etc

We have thought long and hard about the use of IT at St Osmund's Middle School, and have produced a list of guidance about what we see as safe and responsible use. This list has been compiled as a result of from parental questionnaires together with external advice.

Please read through these statements to ensure you feel able to follow them. If you have any concerns or suggestions, please discuss them with the Headteacher or the DSL.

IT Use on School Trips

Cameras used on school trips will be provided by the school. Internal memory cards used in these cameras so that pictures will be provided by the school.

On return to school, all pictures / videos taken are to be transferred to the school system (T-drive). Memory cards can then be wiped for future use.

The school also owns a number of iPods for use on school trips. These can be used as a camera and also to update the school Twitter feeds through connection to WiFi. On return to school iPods are to be returned; any photos are to be transferred to the school system T-Drive and the device wiped for future use.

Acceptable Use Policy – Pupils

Article 17: Everyone has the right to reliable information

AGREEMENT FOR USING THE INTERNET

When using computers, iPads and other ICT equipment that allow us access the Internet -

<u>You should **never** do the following things</u>:

- Send rude or unkind messages to others.
- Play about or be silly near the equipment.
  It could get broken.
- Look at somebody else's work without their permission.
- Waste your computer time, by not completing the task you have been set.
- Tell anyone your personal information or password without checking with a teacher.
- Access inappropriate, offensive or blocked websites.
- Bring in USB sticks, programs or discs from home; this is to prevent data corruption and avoid viruses on the school network.

<u>You should **always**</u>:

- Ask your teacher before you copy things (such as pictures or words) from the Internet.
- Tell your teacher if you see bad language or rude pictures on the computer.
- Make sure that a teacher or adult is present when you are using the Internet.
- Use the school's ICT facilities for school related work.

This agreement is here to protect you and the equipment

**If you break the rules you will not be allowed to use ICT equipment and use the Internet until you can show you can work sensibly and responsibly.*

I have read and understand the School rules for responsible e-Safety, and agree to comply with them. I will use the Internet, e-mail and other IT facilities at school in a safe and responsible way and observe all the restrictions explained to me by the school.

I understand that my use of IT will be monitored and that my parent / carer will be contacted if a member of school staff is concerned with my e-Safety

Pupil's signature.....

Parent's signature.....

Date .....