ST MICHAEL'S
Church of England High School

E-Safety Policy

"What does the Lord ask of you? To act justly, to love mercy and to walk humbly with your God."
(Micah 6:8)

ST MICHAEL'S
Church of England High School

Contents

Statement of Intent

In our school, our Christian vision shapes all we do. All members of the school community are committed to upholding the St Michael's Church of England Christian values:

- to show love, care and kindness to all in our community
- to value what we have and to share with others
- to enable everyone to achieve their full potential

We want all our students to become:

- successful learners, who enjoy, progress and achieve
- confident individuals, who live safe, healthy and fulfilling lives
- responsible citizens, who make a positive contribution to society

Therefore we want our learners to:

- achieve the highest standards possible at Key Stage 3 and 4
- be more skilful at reasoning, information processing, enquiring, creative thinking, evaluating and problem solving
- develop the skills to become more creative and reflective learners and to be effective self-managers
- be more effective participators in the local and global community
- be more engaged and better motivated and see the relevance of their learning in modern society

The whole school E-Safety Policy is linked to the school's aim of ensuring that all students live safe lives.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Date of approval	April 2013
Date of review	October 2018
Review date	January 2020

1. Context

1.1 E-Safety and Safeguarding

The E-Safety Policy is an aspect of the school's Health and Safety Policy and both policies form part of the school's overall Safeguarding Policy. Safeguarding is defined in the Children Act of 2004 and the government guidance document Working together to safeguard children in terms of:

- Protecting children and young people from maltreatment
- Preventing impairment of children and young people's health or development
- Ensuring that children and young people are growing up in circumstances consistent with the provision of safe and effective care
- Undertaking that role so as to enable those children and young people to have optimum life chances and to enter adulthood successfully.

Safeguarding is a key statutory duty for the school and links to the school's aim of ensuring that students live safe and fulfilled lives.

1.2 e-Safety and Anti-Bullying

The E-Safety Policy has links with the schools Anti-Bullying Policy since breaches of the E-Safety Policy could involve bullying of others.
See Appendix 1 Anti-Bullying Policy

1.3 Governor and Staff Involvement

St Michael's Church of England High School Governing Board has fully delegated committees that meet regularly and report back to the full Governing Board. Two committees have responsibility for aspects of safeguarding and the Governors' Chairs' Committee has overall responsibility for the monitoring and evaluating the effectiveness of the school's response to safeguarding.

1.3.1 Health and Safety Committee

The Health and Safety Committee has the responsibility for monitoring and evaluating the E-Safety Policy as part of their remit for health and safety within the school. The named governor for health and safety including e-safety is Clive Priest. He will work with the designated senior member of staff for e-safety to ensure that the annual check list for e-safety is tabled and addressed once a year.
See Appendix 2 Annual checklist for e-Safety Governor

1.3.2 Pastoral Team

The Pastoral Team has to deal with cases where the E-Safety Policy is breached by students as part of an overall serious bullying issue and action has to be taken. The school's designated child protection officers are: Mrs C Hill, Mrs J Mills and Mrs J Gray. Otherwise, incidents of bullying involving e-safety breaches are dealt with by school pastoral staff, inclusion staff and Mr W Hill. Other technical breaches not involving bullying are dealt with by the respective departments.

Mr W Hill [Assistant Headteacher] has been nominated as the e-safety co-ordinator. He is a member of the Health and Safety Committee and will advise the Pastoral Committee as the need arises.

1.3.3 The Network Manager

The Network Manager is responsible for monitoring the school's ICT systems to ensure compliance with the E-Safety Policy and alerting senior managers in the event of a security or compliance breach. He reports on e-safety matters to Mr W Hill [Assistant Headteacher]. Both the Network Manager and the SLT link have attended Securus e-monitoring solution training in November 2013.

1.3.4 The E-Safety Committee

This committee meets to discuss any e-safety issues that the school may have, any action needed to be taken and training for students, staff and Governors. The committee includes the e-safety co-ordinator, e-safety Governor, Network Manager, Head of ICT, teaching staff and representatives from Student Voice.

1.4 Parental Involvement

The Acceptable Use of the Internet Policy (AUP) along with School Rules and Procedures regarding the use of computer equipment are published on the St Michael's Church of England High School website. The E-Safety Policy is available on the school's website.

1.5 Parents and Governors

Parents' and Governors' roles and responsibilities regarding e-safety are outlined in this policy. The AUP is published on the St Michael's Church of England High School website and is issued annually to parents with each pupils Internet Permission Form. Parents and Governors are advised to visit the www.thinkuknow.co.uk website, which explores some of the specific dangers that children could face and provides practical guidance that should make online activity safer for all. We also publish e-safety information for parents on the school website.

1.6 Community use and visitors

Where ICT or other relevant facilities are booked for the use of the community or visitors, they will be asked to sign the Acceptable Use Policy and will be informed that their use will be monitored in the normal way. Visitors must also agree to the code of conduct which is displayed during as user's logon to the network.

Appendix 3 St Michael's Church of England High School Code of Conduct for Visitors
Appendix 4 Code of Conduct for the use of the School Network and the Internet

2 e-Safety Guidelines

2.1 Introduction

St Michael's Church of England High Schools E-Safety Policy covers the safe use of:

- ICT Facilities
- E-mail
- Internet Use
- Mobile Devices

2.2 Access to ICT Facilities

All students and staff at St Michael's Church of England High School have access to ICT facilities with their own personal account and password through SIMS ID. They also have access to the Internet for use in supporting their studies and professional communication. Parental permission is required before students are allowed to access the Internet. Staff and students must sign to agree to the AUP before access is granted; this agreement is reviewed annually.

2.3 Password Security

Everyone has their own user account and private password to allow logon the Internet and email accounts. Administration passwords are used responsibly. Any pupils found to be sharing accounts or passwords will have their account temporarily disabled.

2.4 Code of Conduct for the Use of the School Network and the Internet

Students and staff must agree to accept the rules for the use of the ICT facilities each time they log onto the Curriculum Network by clicking to agree to the Acceptable Use Policy. The Acceptable Use Policy is displayed when pupils and staff log on to the Curriculum Network, anyone who does not agree to this policy is not allowed access to the network. This policy is reviewed annually.
Appendix 4 - Code of Conduct for the use of the School Network and the Internet

2.5 E-Safety Guidelines for Students

Pupils understand what safe and responsible online behaviour means, guidelines are laid out in the AUP. e-safety rules are displayed all rooms where computers are used. Students receive e-safety training as part of the curriculum.

2.5.1 ICT Acceptable Use Policy

The ICT Acceptable use Policy for students is published in the New Intake Booklet and on the St Michael's Church of England High School Website. Students are expected to follow the rules which are set out in the ICT Acceptable Use Policy at all times. Internet and Email use is closely monitored. Appendix 5 -Acceptable Use Policy for Students Appendix 6 -ICT Suite Acceptable Use Policy

2.5.2 ICT Acceptable Use Policy General Rules

Remember always; treat others as you wish to be treated. The use of abusive, racist or intolerant material is not allowed. The following are not permitted:

- Sending, displaying, sharing or downloading offensive messages or pictures;

- Using obscene language;
- Posting malicious or false information about others;
- Harassing, insulting or attacking others;
- Damaging or attempting to damage computers, computer systems or computer networks;
- Violating copyright laws (e.g. downloading copyright protected music, videos or images etc.) without the express permission of the copyright holder;
- Using others' passwords to gain access;
- Sharing of passwords to circumvent restrictions placed on other users;
- Intentionally wasting resources;
- Intentionally denying access to resources by others;
- Sending personally identifiable information to other online users without explicit permission;
- Accessing websites with the intent to access "chat-rooms" or unsupervised e-mail facilities.

2.6 Internet Permission Form and Parents Guide to the use of the Internet

An Internet Permission Form and Parents' Guide to the use of the Internet are sent to all parents at the beginning of each school year. This also provides information of the School Rules and Procedures regarding the use of computer equipment. Students are not provided with Internet access until the Internet permission from is returned to school having been signed by a parent and pupil. Internet permission forms are held by the ICT Department

Appendix 7 – Internet Permission Form

Appendix 8 – Parents' guide to the Use of the Internet

2.7 Inappropriate Websites

Sites which give access to the following types of material are not allowed:

- Drugs and substance abuse (educational sites are allowed)
- Pornography and age restricted sites
- Intolerant Behaviour
- Proxy By Pass
- Violence
- Social networking
- Web based chat
- Web based mail (pupils only)
- Non educational games
- Mobile Phones/ringtones
- Executable downloads
- Mp3 downloads

A filtering service provided by TRUSTnet which uses a bespoke web filtering system, WebScreen™ 2.0, is tailored to meet the needs of schools and offer a high degree of flexibility to each one. Filtering occurs from the moment of connection, with each school having full access to the configuration settings. WebScreen™ 2.0 allows each school to create the filtering environment best suited to all its different types of users. The system filters by IP address groups as a default, with Per-User filtering being an option that can be activated by the school at any time. Time-based filtering is another feature that aids flexibility so that filtering policies can be adjusted automatically for

different users at different times of the day. This centrally-deployed system maximises performance with no proxy-related delays and no hardware to worry about. All filtering is Internet Watch Foundation compliant with further e-safety guidance available from TRUSTnet. A number of other safety precautions are also in place to protect schools from a range of online hazards but the majority of settings are placed directly within the school's control. Internet access is closely monitored by the ICT Department, who also maintain in-house filter lists. The filter list has been designed to reflect educational objectives and has been approved by the Headteacher. If an inappropriate website if found accidentally it should be reported to the ICT Department for investigation.

Misuse of the Internet is dealt with following the procedures laid out in the BECTA publication "What to do with Suspicious Web Browsing" [Appendix 8] and the procedure outlined by the Sandwell Local Safeguarding Children's Board [Appendix 9]
Appendix 9 – BECTA Publication –What to do with Suspicious Web Browsing
Appendix 10 - Sandwell Local Safeguarding Children Board

2.8 Sanctions
Should a student be found to have breached any of the rules then an appropriate sanction will be applied. Sanctions include:

Type of Site	**Action Taken**
Games sites during lesson time	2 week Internet ban, after school detention & letter to parents
Social networking	2 week Internet ban, after school detention & letter to parents
Glamour	3 week Internet ban, after school detention & letter to parents
Pornography	12 week Internet ban, after school detention & letter to parents
Intolerance	12 week Internet ban & letter to parents
Gambling	12 week Internet ban & letter to parents
Proxy By Pass	12 week Internet ban & letter to parents
Illegal Sites	Reported to the police for investigation
Bullying via email messages, social media or any other form of digital media	Reported to Pastoral Staff for further action potential police investigation

Where e-safety has been breached and this is linked to bullying behaviour, this will be referred to the Pastoral Team for further action. The Internet logs are regularly monitored and sanctions are applied where necessary. An incident log is maintained in the ICT Department.

2.9 Email

Everyone who has signed the Internet Permission Form is allowed to send emails and attachments to outside recipients. A banned word filter list is in place which redirects filtered mail to the Administrators email account and notifies the sender. Pupils who send emails which containing bad language have their email access temporarily banned. Any evidence of bullying via email is referred to the Pastoral Team and dealt with accordingly.

2.10 SMART Rules

Pupils should be aware of the 5 SMART Rules which are published by Childnet International:

S Safe: Keep safe by being careful not to give out personal information such as your name, email address , home address, school name, phone numbers and photographs.
M Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's or carers consent and only when they can be present.
A Accepting: Accepting emails, instant messages, files or texts from strangers can lead to problems.
R Reliable: Information you find on the Internet may not be true, or someone online may be lying about who they are.
T Tell: Tell your parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried or if someone you know is being bullied online.

e-safety posters are also displayed in classrooms. SMART Rules are published in the homework planners.

2.11 E-Safety Assemblies

E-safety assemblies are delivered to students where the guidelines for are reinforced and the schools stance against any form of bullying is reinforced.

2.12 Mobile Devices

Students are allowed to bring mobile phones into school but are not allowed to use them in the classroom or inside the school building. If they come to the attention of a member of staff, they are confiscated and given to the school office for return at the end of the school day. If the problem is repeated, the parent will be required to come into school to collect the phone from the office.
Any misuse of mobile phone technology e.g., photos, abusive text messages, social media and video clips are dealt with by Pastoral Staff as part of an anti-bullying policy.

2.13 Photographs and video imaging

The school follows Sandwell LA guidelines regarding the use of photographs and video images in school and new parents' are asked to indicate if they do not want photographs or video images taken of their child as part of the new parent induction pack.
Appendix 10 - Guidance for Schools Using Digital Images of Children & Young People, Sandwell Council
Appendix 12 - Photograph consent form

3 E-Safety Guidelines for Staff

Staff have an understanding of e-safety issues and risks, guidelines are laid out in the staff IT Policy. Staff receive training and updates as appropriate. New teaching staff receive e-safety training as part of their induction process.

Issues of concern are escalated following the procedures outlined in the BECTA publication 'What to do with Suspicious Web Browsing', and the procedure outlined by the Sandwell local safeguarding Children's Board [Staff receive regular Child Protection training and know how to conduct themselves professionally online].
Appendix 9 - BECTA Publication - What to do with Suspicious Web Browsing
Appendix 10 - Sandwell Local Safeguarding Children Board

3.1 ICT Security Guidelines and Rules for Staff

All members of staff are issued with a copy of the IT Policy which detail the rules for both the curriculum and administration networks. Signed copies to show compliance to the agreement are held by the ICT Department. The IT Policy is reviewed annually.
Appendix 14 – Acceptable Use Policy - Staff
Appendix 15 – Acceptable Use Policy – Staff Declaration

Any member of staff found to be using the Internet inappropriately will be reported to the Headteacher or to the police if the site contains Illegal content.

3.2 Sanctions

Staff [teaching or non-teaching] who misuse ICT in the school and breach the school's E-Safety Policy are subject to sanctions which include:

- Removal of access to ICT facilities
- Disciplinary warnings [in line with the LA disciplinary policy]
- Dismissal [in line with the LA disciplinary policy]

4 Security

4.1 Access to Digital Communications and Technologies

Levels of access to the both the administration and curriculum network are controlled by the use of user types.

4.2 Antivirus

The curriculum network uses Broadband Sandwell software, the administration network also uses Broadband Sandwell software both of which are updated regularly. The antivirus software is set to automatically scan memory sticks and other portable devices. All laptops have antivirus software installed which is set to update automatically and to scan memory sticks and other portable devices. The network is not setup to automatically scan laptops.

4.3 Securus Monitoring Solution

A Securus Sever is used to monitor all ICT activity on the Network. Mr W Hill [Assistant Headteacher is the Securus Server Administrator and the Securus Management Supervisor. Logs are checked daily and any misuse is reported to the Senior Leadership Team, Head of ICT or Pastoral Team for further action. Incidents of misuse are recorded by the ICT Department. Mr W Hill attended Securus e-monitoring solution training in November 2013.

4.4 Filtering

TrustNet Broadband Filtering is used to prevent access to the following types of websites:

- RM IWF Child Abuse Images List
- Sandwell LA Filter List
- RM Web-Based Social Networking List
- RM Web – Based Chat List
- RM Non Educational Games List
- RM Pornography or Age Restricted Activity List
- RM Violence List
- RM Intolerance List
- RM Drugs and Substance Abuse List
- RM Proxy Bypass List
- RM Active - Adapt Content Filter List

4.5 Caching Server

A Caching Sever is in use so that all computers access the Internet via the Cache. The Caching Server is used to filter Internet content in accordance with the E-Safety Committees recommendations.

4.6 Video Conferencing

Video conferencing is not used at present. The school is aware of the need to use the national JVCS service to check that connections are made to legitimate sites.

4.7 Internet Services

A BECTA accredited supplier is used to provide Internet Services.

4.8 SEF

e-safety measures are included in Section 4b of the schools SEF.

4.9 Cyberbullying

This is covered in the school's Anti-Bullying Policy.
Appendix 1-Anti-bullying Policy

4.10 Data security

There is a planned outline for staff training on data security and new staff have e-safety training as part of their induction. From September 2017, the school will use a terminal server and Go for Schools which allows staff to access data at home without having to store it on memory sticks. In

staff training, staff are aware the do's and don'ts on saving data and when and where to access information. The school follows Sandwell's LA guidelines on data security.

4.11 Privacy Notice

Privacy Notice -Data Protection Act 1998 St Michael's Church of England High School is the Data Controller for the purposes of the Data Protection Act; a Privacy Notice is displayed on the St Michael's Church of England High School Website.

Appendix 13 – Privacy Notice

5 Audit

The school Assistant Headteacher and ICT Department complete an annual audit of compliance with ICT security guidelines. This is produced by the South West Grid for Learning. The audit can be found at http://www.learn-ict.org.uk/self_review/docs/swgfl_esrf.pdf.

Appendix 1 Anti-Bullying Policy

ST MICHAEL'S
Church of England High School

Anti-Bullying Policy

Date adopted	November 2008
Date revised	5th October 2017
Next revision date	October 2018

Contents

Statement of Intent

St Michael's Church of England High School will not tolerate bullying of any kind and will deal with any reported incidents promptly and effectively. Support and counselling will be offered to the victim and strategies to deal with the bully will be sought. Issues relating to bullying are regularly discussed in PSHE, appropriate lessons, assemblies as well as other forums. A 'pupil speak' version of this policy will be issued to all pupils.

This policy aims to:

- develop a culture where bullying will not be tolerated and any incident of bullying can be reported
- encourage pupils to support each other and be actively involved in making the school a bully-free zone
- work closely with pupils, parents, staff and outside agencies to minimise incidents of bullying
- involve Student Voice in developing and implementing this policy
- provide pupils with the opportunity to make a positive contribution and achieve emotional wellbeing by creating a safe and healthy environment

Signed by: _____ Date: _____

Headteacher

Signed by: _____ Date: _____

Chair of Governors

Bullying

Definition

A repeated act which is often deliberate causing distress to the victim. This may be the result of a thoughtless act, or a wilful and conscious desire to hurt, threaten or frighten.

Types of Bullying

There are many different types of bullying that children may. Some may be obvious to identify, whereas others may be more subtle. Some of the ways that bullying may be identified could be as follows:

- Physical
- Verbal
- Social
- Cyber

Physical Bulling

Physical bullying is often the most obvious and easily identified. Physical bullying includes; hitting/punching, kicking, tripping, pinching, pushing, nudging. Physical bulling can cause both short term as well as long term damage and in turn may also harm a child's emotional well-being even once all physical bulling has diminished.

Verbal Bullying

Verbal bullying includes; insults, name calling, intimidation, teasing, homophobic/cultural/sexist or racist remarks. In some instances the above may begin harmlessly but it can soon escalate to levels which start to affect an individual's emotional well-being and this may become verbal abuse.

Social Bullying

Social bullying is often identified as being the hardest type to identify and is sometimes recognised as covert bullying. It is often harder to recognise as this type of bulling may be carried out without it being directed at the victim (in other words, behind the bullied person's back). This type of bullying is often with the intent to harm an individual's social reputation and/or to cause humiliation. Social bullying may include:

- Lying to and/or spreading rumours
- Negative physical or facial gestures, threatening or disrespectful looks
- Ignoring a person or group intentionally
- Socially excluding someone and/or encouraging others to socially exclude someone
- Intentionally damaging someone's social reputation and/or social acceptance
- Intending to embarrass or humiliate someone i.e. mimicking, obscene gestures

Cyber bulling

Cyber bullying can often be identified as either or both, obvious or secretive forms of bulling that take place using digital technologies, including; mobile phones, IPad's/tablet's, computers and/or using software such as social media, instant messaging, websites, text messages and other online platforms. Cyber bulling can happen at any time. It can be in public or in private and sometimes is only known to the person being bullied and the person bulling. Cyber bullying may be identified as follows;

- Abusive and/or hurtful text messages, emails, posts, images and/or videos

- Hurtful gossip and spreading of rumours online
- Imitating other people online and/or using their account/log in
- Deliberately excluding people online

There has been a dramatic increase in the use of chat rooms, social media and instant messaging by teenagers. These include Facebook, Instagram, Snapchat, Messenger etc. The school will endeavour to use assemblies, PSHE and form time to highlight and make pupils aware of the issues involved with chat rooms and e-safety. The school will take the use of these sites to bully very seriously and will thoroughly investigate problems that arise. Where possible, training and information raising will also take place with parents.

Symptoms of Bullying

Some pupils will openly raise their concerns about being bullied. However, others may be unwilling to talk about it for fear of not being understood and making the situation worse.

Parents or carers may notice signs such as:

- Bed wetting in a previously dry child
- Vague tummy aches and headaches
- School refusal/reluctance to go to school
- Being frightened of walking to and from school or changing their usual route
- Arriving home with books or equipment missing
- Arriving home hungry because lunch money has been taken
- Becoming withdrawn or lack in confidence
- Becoming distressed and anxious

School staff may notice:

- A decline in the standard of work
- Poor punctuality/attendance or truancy
- Falling out with a previously good friend
- Unexplained bruises, cuts or scratches
- The pupil becoming aggressive and unreasonable
- Reluctance to go out at break or lunch
- Hanging around classes with the excuse of staying to help

Rights and Responsibilities

- It is the right of all pupils in the school to be free from humiliation, fear and abuse. It is therefore the responsibility of all adults and pupils in the school to ensure that the atmosphere for learning is caring and protective.
- All teaching and non-teaching staff, pupils and parents should be involved in implementing the Anti-Bullying Policy
- The PSHE programme, assemblies and School Council will inform pupils and staff of the procedures that are in place to combat and deal with bullying
- All vulnerable areas of the school should be visited on a regular basis by all staff
- All teaching and non-teaching staff should demonstrate understanding of pupil's feelings and be aware that sometimes throw-away comments may make a situation worse
- All staff should act swiftly when incidents of bullying are reported
- Pupils should be allowed the opportunity to discuss their worries and fears about any aspect of school life. This can be done through the strong support networks that are in place including the School Council, peer mentors, learning mentors and other staff

Guidelines

Pupil Guidelines

- If pupils are being bullied, or may know someone that is being bullied, they should be encouraged to tell someone. There is a range of staff that pupils can see:
- Subject teacher
- Form Tutor
- Assistant Head of Year
- Head of Year
- Pastoral Support Staff
- Senior Staff (Assistant Heads, Deputy Head Teacher, Head Teacher)
- Academic coaches
- Admin staff/school nurse/lunchtime supervisors

Pupils can also tell friends, peer mentors or prefects if they are being bullied, who should pass the information on to a member of staff.

Staff Guidelines

- All staff share a responsibility to create a safe, enjoyable and trusting atmosphere where pupils can achieve and feel confident to talk to any teacher or other trusted adult and share with each other concerns that they may have
- Staff should report incidents of bullying to the appropriate Pastoral Head or Senior Leader
- Use the form tutor time as positive support against bullying, reminding pupils what to do as often as possible
- Pupils should receive guidance through PSHEE, assemblies and School Council about the different forms of bullying and what to do if they are a victim of bullying
- Pupils need to be taken seriously when disclosing incidents of bullying and should be seen as soon as possible to discuss it
- If bullying is suspected, the victim should be spoken to and offered support and advice
- Reinforce the school's policy on bullying wherever possible
- Use the school's policy on bullying wherever possible
- Use the school's referral system to inform other staff about incidents

When dealing with any form of bullying, the action taken will follow Ofsted guidelines, 'swift, proportionate, discreet, influential and effective. The victim must feel confident that the situation will be resolved effectively. Bullying will be reported through the school's referral system on SIMS/ Go 4 Schools. This will be recorded by any member of staff who deals with the issue. Incidents will be recorded appropriately and will be reported to the Governing Body.

Governor Guidelines

There may be situations where parent governors are made aware of bullying incidents. The following procedures should be followed:

- Governors should encourage parents to speak to the appropriate head of year to resolve the situation in the first instance.
- Make a telephone call to the appropriate Head of Family to inform them of their contact with parents.
- If the bullying has not been resolved, the governors should contact the Head Teacher or Associate Head Teacher, who should report back once the issue has been resolved.

Parent Guidelines

Parents are in a prime position to pick up the early warning signs that their children may be the victims of bullying. If parents are concerned that their children are being bullied, they should contact the relevant Pastoral Head immediately. Often incidents can be dealt with before they get out of hand, so that they are brought to a swift conclusion.

Parents know their children better than anyone else. Any changes in behaviour or attitude towards school which is not in the child's usual manner, may be warning sign that bullying is taking place.

Where possible parents should monitor their child's use of social networking sites such as Facebook. Parents should check on a regular basis the content of what is being said and take appropriate actions. This should include informing the school.

Procedures

The definition of bullying at the start of the policy makes it clear that bullying is a repeated act, therefore, 'one-off' incidents such as fights are not deemed as 'bullying'. However, these incidents will be recorded on SIMS. The situation will be closely monitored in case they become more serious. Serious incidents will be dealt with by Head of Year (HoY) or a member of Senior Leadership Team (SLT).

Where a member of staff is concerned that bullying is taking place, they should gain as much information as possible and pass it on to the HoY or member of SLT. Any information should be recorded on SIMS. The following strategies may be used during any investigation and preventative work. The strategies employed will depend on the seriousness, frequency and type of bullying. It will also depend on whether the bully has been involved in other bullying. If an incident were to arise, the school would typically investigate and resolve as follows;

- Pupil interview/ Incident Report/ Statements
- Parental involvement: Contact with Parent/Guardian
- Letter home
- Discussion with /Support for the Victim
- Discussion with and Verbal warning to the bully, information placed on file
- Consequence
- Letter of apology
- Involvement of Assistant Head of Year/ HoY, Pastoral Support Team and Outside Agencies
- Fixed Term or Permanent Exclusion from school
- Use of outside agencies (including the police)

The level of severity of an incident, will determine what processes are required to support and resolve the situation. However, in all cases the incident details should be recorded on SIMS by the

investigating person(s).

Support for the Victim

The pastoral system is structured in such a way as to offer considerable help and support to the victims of bullying. The wealth of experience of Pastoral Staff will be used to help and support such victims, so that they feel safe and secure in school. The key to this is the partnership between parents, pupils and school.

Support for the Bully

It is often forgotten that there may be a reason why a person targets others and displays bully-like behaviour. Sometimes, bullies may not even recognise themselves that they are in fact causing harm or portraying bully-like behaviour. In some cases students do not accept that their behaviour is unacceptable. In other cases, they may themselves once have been the victim of bullying, or may have grown up within that environment. With this in mind, bullies may also need help and support so that they modify their ways and become responsible for their own actions and others' rights. The following help is available for students who display bully-like behaviour;

- Emotional and Social well-being support i.e. Counselling, Referrals to external agencies
- Peer/ Relationship Restorative Intervention
- Involvement from External agencies
- Parental support and involvement
- Alternative provision

Appendix 2: Annual checklist for e-Safety Governor

It is the responsibility of the e-Safety Governor to ensure that this document is tabled once a year at the termly meeting of the full Governing Board and at the next meeting following any major incident.

Action	**Completed by: (date)**
The Acceptable Use Policy (AUP) is in place and has been revised to accommodate any developments in technology and its use	
All staff (teaching and non-teaching) and any volunteers or supply staff are familiar with the current E-Safety Policy and the AUP	
e-safety forms a part of the induction process for all new staff	
All new parents/carers have received a copy of the school's AUP	
All parents/carers have received a copy of the Internet access permission form and returned their response to school	
All staff (teaching and non-teaching) and any volunteers or supply staff are in possession of the 'A concern is raised' flow diagram and now what to do if an incident occurs	
All users are compliant with additional AUPs and terms and conditions contained I n other services (such as a learning platform) and procedures are in place to ensure this happens	
All users understand the use of e-safety monitoring software were installed	

Chair of Governing Body:

_____ Date: _____

Note: The Governing Board should be aware that it is a duty of Sandwell Metropolitan Borough Council to monitor the processes outlined above and this document should be retained in order to facilitate that process.

Appendix 3: St Michael's Church of England High School Code of Conduct for Visitors

You must read, understand and sign this form if you use our ICT facilities and services. The completed form will be retained by the ICT Department.

The following are not permitted:

- Sending, displaying, sharing or downloading offensive messages or pictures;
- Using obscene language;
- Posting malicious or false information about others;
- Harassing, insulting or attacking others;
- Damaging or attempting to damage computers, computer systems or computer networks;
- Violating copyright laws (e.g. downloading copyright protected music, videos or images etc.) without the express permission of the copyright holder;
- Using others' passwords to gain access;
- Sharing of passwords to circumvent restrictions placed on other users;
- Intentionally wasting resources;
- Intentionally denying access to resources by others;
- Sending personally identifiable information to other online users without explicit permission;
- Accessing websites with the intent to access "chat-rooms" or unsupervised e-mail facilities.

Use of the school's ICT facilities and Internet is closely monitored. Should anyone be found to have breached any of the rules, an appropriate sanction will be applied. Sanctions include:

- A temporary or permanent ban on ICT equipment, Internet and/or e-mail use;
- Where the action originated outside the school premises, a formal request to the Internet Service Provider (ISP) requesting the termination of the service and account(s) of the publisher and/or author will be issued;
- Where applicable, the matter may be referred to the police or other local authorities.

Declaration

I confirm that, as an authorised user of the school's ICT facilities, e-mail and Internet services, I have read, understood and accepted all of the rules for visitors.

Name:_____ Signature:_____

Date:_____

Appendix 4: Acceptable Use Policy

Code Of Conduct For Use Of The School Network & The Internet

This simplified code of conduct applies at all times, in and out of school hours, whilst using school equipment.

Please read it carefully.

You should:

- Only access websites that are appropriate for use in school.
- Be careful of what you say to others and how you say it.
- Respect copyright and trademarks. (You cannot copy material without giving credit to the person or company that owns it.)
- Check with a teacher before opening email attachments or completing on-line questionnaires or subscription forms.

You must not:

- Download games or other programs from the Internet.
- Use chat-lines or web-based email services (e.g. Hotmail).
- Send, access or display offensive messages or pictures.
- Give your name, address, telephone number or any other personal information about yourself or others to anyone you write to.
- Use or send bad language.
- Intentionally waste resources thus preventing use by others.

Please note:

User areas on the school network will be closely monitored and staff may review your files and communications to maintain system integrity. Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved, as certain activities may constitute a criminal offence.

Appendix 5: ICT Acceptable Use Policy (AUP) Policy Statement

As part of the school's IT programme we offer pupils supervised access to the Internet, the global network of computers you will have read about and seen on television. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter. Access to the Internet will enable pupils to explore thousands of libraries, databases and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some.

All activity on the computer system is logged, in particular the students' use of the Internet; these activity logs are closely monitored and frequently reviewed. The Internet activity logs store a variety of information, including: the user identity of the student, the date and time of access, the computer used by the student and the Internet address of every page and image that was accessed. In addition, e-mails are routinely scanned for offensive language by the computer system and, any that "fail" this preliminary scan are redirected to the I.T. Coordinator for further scrutiny. Access to websites providing external e-mail accounts are blocked, allowing the school to ensure and enforce the appropriate use of e-mail via the school's computers.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. Whilst the school will endeavour to "police" the use of the Internet in school, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Parents are advised to visit the following website www.thinkuknow.co.uk, which explores some of the specific dangers that children could face and provides practical advice and guidance that should make the online experience safer for all.

School Procedures

Resource Development

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer "home pages" and menus of materials that are appropriate to the age range and ability of the group being taught. The IT co-ordinator will provide appropriate guidance to pupils as they make use of telecommunications and electronic information resources to conduct research and other studies. All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group. As much as possible, the school's chosen information provider has organised information resources in ways that point pupils to those that have been reviewed and

evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Pupils may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

School Rules

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all pupils, and kept under constant review. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

Every year students will be required to complete a Parent & Student agreement Form regarding the use of the Internet which outlines the AUP of the school. In addition, students are required to reaffirm their agreement, to follow the AUP, every time they login and every time they attempt to access the Internet and/or e-mail systems. The agreement form will be issued by form tutors during the first couple of weeks of every new academic year. Internet access will be removed for any student who does not have a current agreement returned and on file.

Appendix 6: ICT Rooms/ILD usage within departments

Acceptable Use Policy
St Michael's Church of England High School ICT Rooms and ILD's situated in Lap-safes within departments all have Internet access to help users learn.

These rules will help keep everyone safe and help us be respectful of other users. **Remember always treat others as you wish to be treated.**

The use of abusive, racist or intolerant material is not allowed.

- I will only access the system with the login and password provided
- I will not access other people's files
- I will only use the computers for work related activities
- I will not use the CD's or other computer media unless I have been given permission.
- I will ask permission from a member of staff before using the Internet
- I will only e-mail people I know for work/learning related purposes
    - The messages I send will be polite and responsible
- I will not give out personal information
- I will use Ctrl Alt Delete to lock my workstation when leaving it unattended
- I will report any unpleasant material or messages I find or are sent to me
- I understand that there will be checks and monitoring of the computer use and Internet sites I visit
- I understand reports will be confidential and will help protect myself and others

Pupil Signature _____ Date ___ /___ /_____

Name of Pupil _____ Form _____

Appendix 7: Internet Permission Form

Dear Parent,

As part of the school's IT programme we offer pupils supervised access to the Internet, the global network of computers you will have read about and seen on television. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter. Access to the Internet will enable pupils to explore thousands of libraries, databases and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some.

All activity on the computer system is logged, in particular the students' use of the Internet; these activity logs are closely monitored and frequently reviewed. The Internet activity logs store a variety of information, including: the user identity of the student, the date and time of access, the computer used by the student and the Internet address of every page and image that was accessed. In addition, e-mails are routinely scanned for offensive language by the computer system and, any that fail this preliminary scan are redirected to the IT Coordinator for further scrutiny. Access to websites providing external e-mail accounts are blocked, allowing the school to ensure and enforce the appropriate use of e-mail via the school's computers.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. Whilst the school will endeavour to "police" the use of the Internet in school, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Parents are advised to visit the following website www.thinkyouknow.co.uk which explores some of the specific dangers that children could face and provides practical advice and guidance that should made the online experience safer for all.

We would be grateful if you would read the outline acceptable usage policy overleaf and, if you wish to allow your child to access the Internet, then complete the permission form that appears at the bottom of this page. Any student who does not have a permission slip on file with the IT office will have their Internet and email account disabled; they can be re-activated at any time upon the return of the permission slip.

Yours faithfully,
Mrs J Gray, Head Teacher

Please complete and return this consent form to the Headteacher via your child's form tutor.

Pupil

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil Signature _____ Date ___ /___ /_____

Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent Signature _____ Date ___ /___ /_____

Name of Pupil _____ Form _____

Appendix 8: A parent's guide to the Internet

What is the Internet?
The Internet is a large number of computers all over the world linked together with cables. In most cases, each of these computers is also linked locally to a number of other computers, in a local network.

It is possible for someone using one of these computers to access information on any of the other computers. Universities and Government organisations established the system for the fast and efficient transfer of largely text-based information around the world directly from one computer to another. It is possible for other people, outside these local networks, to connect to the Internet by using standard telephone lines between their computers and those already connected to the Internet. A number of companies specialise in providing this service for a fee.

What is the world wide web?
To make the appearance of information available through the Internet more attractive, and to assist people in finding information more easily, it is now possible for special pages of information to contain text, colours, and pictures, sound and even video. These pages, collectively, make up what is known as the World Wide Web. Most of these pages include information on the location of other pages on the World Wide Web, and it is possible to follow up links between pages with similar or related content. Moving from one page to another, regardless of where in the world they might be located, is called browsing, or surfing the net or web. Many of these Web pages contain information that may be useful in the classroom, and it is presented in a way that is often easy to use.

A number of UK suppliers including BT and Research Machines, offer schools the facility of keeping their own pages on the Internet. These school "home pages" might describe the school's activities to outsiders or explain project work that pupils are involved in.

What is electronic mail (e-mail)
This is merely a way of sending messages from one person to another via the Internet. Each Internet user has a unique e-mail address (such as anybody@msn.com) and by sending a message to this address, the recipient can read the message the next time he or she connects to the Internet. Internet e-mail addresses are usually provided along with a schools' connection to the Internet and normally pupils will have their own e-mail address.

What are News Groups?
These are collections of messages written for public readership rather than addressed to an individual. Each collection, or group, of messages is about a particular subject or theme. Individuals can reply to these messages, and these replies are also public. In this way it is possible to track a multi-way conversation about an important issue of the day. At present there are more than 10,000 different topics available for discussion, from specialist science research to support groups for asthma to fans of James Bond movies. Most of the press concern for pornography on the Internet refers to newsgroups but they are the easiest for school Internet providers to police.

What are social network sites?

Sites such as Instagram, Bebo and Facebook allow people to keep in touch with friends using photographs, videos and message boards. These sites are very popular with young people but they do introduce potential risks including cyberbullying, misuse of personal information and contact by adults with a sexual interest in children. Social networking sites provide safety tools which allow the use Privacy Settings. Parents should ensure that these tools are used to which give control of who can see, make comments or copy photographs from their child's social networking site.

What is Cyberbullying?

Cyberbullying is the use mobile phones and the Internet, deliberately to upset someone else. This can take a range of different forms, such as nasty text messages on mobile phones, instant messaging in chat rooms, posting of images or messages on social networking sites or video sharing sites. This type of bullying is particularly distressing as the target can be reached at any time and any distressing material can often be seen by a large audience causing humiliation to the person concerned. Bullying incidents often start off as a joke which quickly gets out of hand, children should be encouraged to always respect others and to be careful of what they say or post online.

What are the dangers of the Internet referred to in the media?

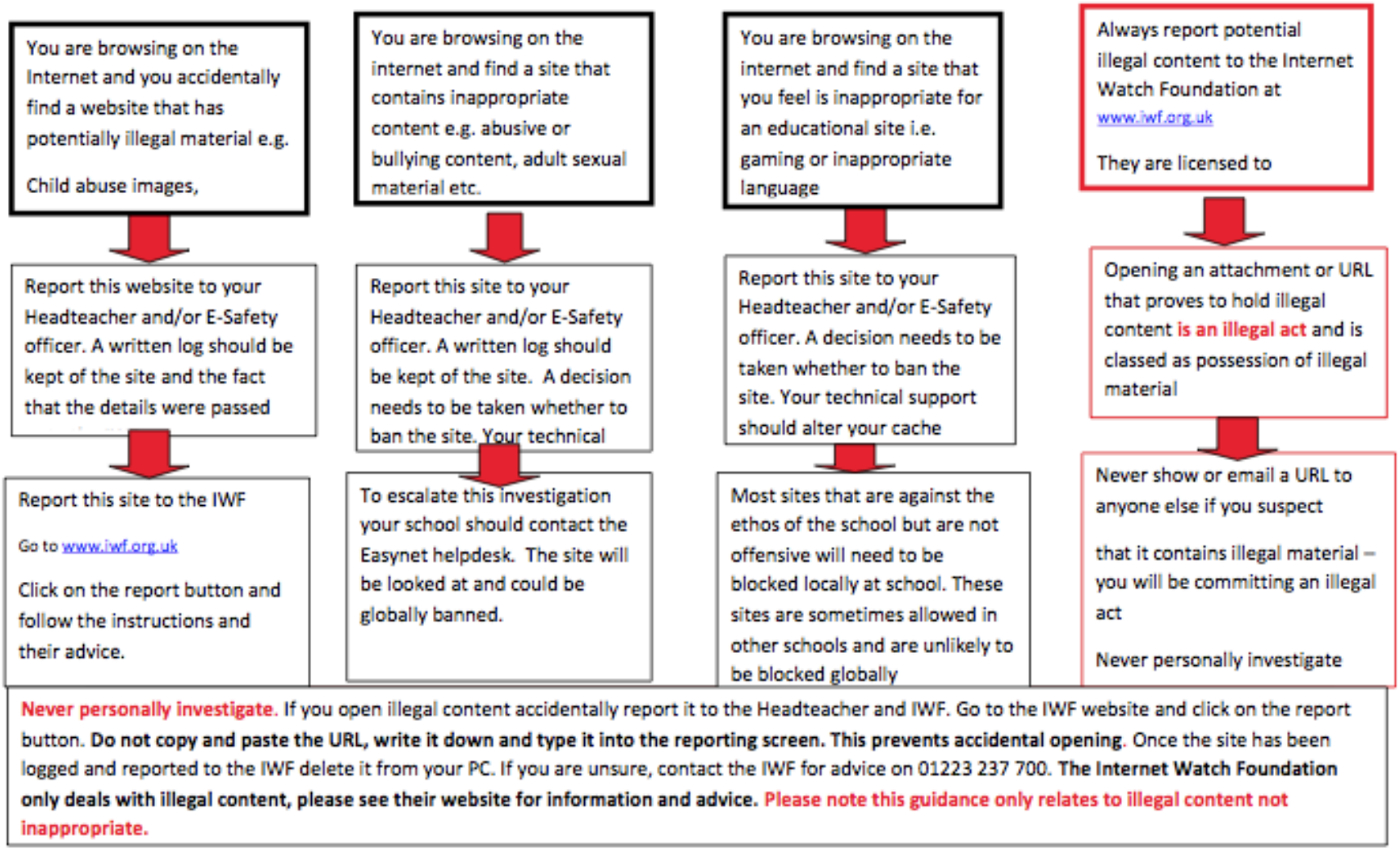
It is true that there is some material on the Internet that would be offensive to most people, such as pornography, racist and fascist material; students, if unsupervised, might access this. The provider that we use tries to 'filter' known offensive locations of material of this kind, but there are too many sites on the Internet for this filtering to be 100% effective. The only guaranteed way to block access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the Internet may be lost. It is a feature of the Internet that the information available is free. Increasing restrictions will undoubtedly lead to systems of charging for access to specific material, in addition to the other costs described. An alternative system is to educate pupils and encourage an acceptable use policy and partnership between home and school in dealing with the less savoury side of Internet use.

How can I get more information?

Parental guidance to safe use of the Internet is available on the www.thinkyouknow.co.uk website. This includes frequently asked questions and guidance about chat rooms, social networking, gaming, mobile phones, grooming and online gaming. There are many magazines in newsagents that cater for beginners-advanced use of the Internet. If you have any specific questions please contact the school and ask for the IT coordinator.

Appendix 9

BECTA Publication - What to do with Suspicious Web Browsing



Never personally investigate. If you open illegal content accidentally report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the site has been logged and reported to the IWF delete it from your PC. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

Appendix 10 - Sandwell Local Safeguarding Children Board

What is the role of a Local Safeguarding Children Board?

A Local Safeguarding Children Board (LSCB) is a multi-agency body set up in every local authority. The LSCB has a range of roles and statutory functions including developing local safeguarding policy and procedures and scrutinising local arrangements. The statutory objectives and functions of the LSCB are detailed below.

Statutory objectives and functions of LSCBs

Section 14 of the Children Act 2004 sets out the objectives of LSCBs, which are:

- to coordinate what is done by each person or body represented on the Board for the purposes of safeguarding and promoting the welfare of children in the area; and
- to ensure the effectiveness of what is done by each such person or body for those purposes

Regulation 5 of the Local Safeguarding Children Boards Regulations 2006 sets out that the functions of the LSCB, in relation to the above objectives are as follows:

- developing policies and procedures for safeguarding and promoting the welfare of children in the area of the authority, including policies and procedures in relation to:
    - the action to be taken where there are concerns about a child's safety or welfare, including thresholds for intervention;
    - training of persons who work with children or in services affecting the safety and welfare of children;
    - recruitment and supervision of persons who work with children;
    - investigation of allegations concerning persons working with children;
    - safety and welfare of children who are privately fostered;
    - cooperation with neighbouring children's services authorities and their Board partners
- communicating to persons and bodies in the area of the authority the need to safeguard and promote the welfare of children, raising their awareness of how this can best be done and encouraging them to do so;
- monitoring and evaluating the effectiveness of what is done by the authority and their Board partners individually and collectively to safeguard and promote the welfare of children and advising them on ways to improve
- participating in the planning of services for children in the area of the authority; and
- undertaking reviews of serious cases and advising the authority and their Board partners on lessons to be learned.

To report a concern about a child, visit the website at http://www.sandwelllscb.org.uk/ or telephone Sandwell MASH on 0121 569 3100.

Appendix 11 - Sandwell Local Authority Guidance – Taking Images of Children

ST MICHAEL'S
Church of England High School

Guidance For Schools Using Digital Images Of Children And Young People

Headteacher: **Mrs J Gray, MSc, NPQH**

St Michael's Church of England High School • Rowley Learning Campus • Curral Road • Rowley Regis • West Midlands • B65 9AN
Telephone: **0121 561 6881** • Fax: 0121 561 6882 • email: contact.staff@st-michaels.sandwell.sch.uk

Contents

This guidance was produced by Sandwell Metropolitan Borough Council.

Guidance for Sandwell Schools

Digital technology has vastly increased the use and potential misuse of photographic images (printed, digital and video images) and concerns about allowing the filming of children & young people's events and publishing their pictures to web sites has highlighted the need for advice that schools should have a consistent, legal and up to date policy about the use of photographic images.

In developing such a policy for your own school we suggest that, head teachers, governing bodies and other managers should open the issue for discussion and explanation with parents and other stakeholders. It should always be possible to enable those parents / staff members with particular concerns to specify that they withhold their consent for whatever reason.

Most abused children are abused by someone they know; the risk of a child being directly targeted for abuse through being identified by a stranger is small. Providing reasonable steps are taken to ensure a photograph is appropriate and the full name and contact details are protected that photography for school and other events by staff, families and the media should be allowed. We are aware that the widespread use of mobile telephones as digital cameras would make banning difficult to impose.

Generally photographs for school and family use and those that appear in the press are a source of pleasure and pride. They usually enhance self-esteem for children and young people and their families and this should continue within safe practice guidelines.

These guidelines attempt to raise awareness of the potential dangers to children whilst offering practical, reasonable and proportional advice to schools and services.

For further guidance relating to data protection issues for schools please see the guidance issued in circular 112 of 27/4/2007.

Please contact the Local Authority Child Protection Officers for Education if you wish to discuss this advice or seek any further help.

1. Issues of Consent

The Data Protection Act 1998 affects our use of photography. An image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent/carer of anyone under the age of 18 years for any photographs or video recordings for purposes beyond the school's core educational function e.g. school web sites, school productions. It is also important to ascertain the views of the child/young person when considering that. The Information Commissioner has suggested that a young person from 12 years old may consent if they are deemed competent.

As it is likely that there will be a number of occasions during a child's educational journey when the school may wish to photograph or video that pupil, we recommend that consent is sought when the pupil starts at the school, to last for the duration of their stay.

There will also be times when off-site activities are taking place e.g. activity holidays or educational visits. In these circumstances it is possible that the school will want to make some visual record. It is also likely that children and young people will want to make their own visual records so it is important that organisations develop policies and guidelines re use of mobile phones with cameras and digital cameras.

For school and other events which are photographed for publicity purposes, a signed consent form should be obtained from the child's parent/guardian or the child and kept on file covering all cases where images of children are to be published beyond the parameters of school use. An example can be found in Appendix B.

Where children are 'Looked After', schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, e.g. adoption placements or following a resettlement from domestic violence, where a child's security is known to be at stake. If there is any indication that a child's security may be compromised advice must be sought.

Consent gained for photographs or videos may not extend to website or webcam use. It is essential that acceptable use policies are in place and consent from the parent/carer is gained to enable children and young people to use these mediums in school.

Parents may withdraw consent to any use of digital medium at any stage; good practice indicates this should be done in writing.

2. Planning Photographs of Children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

- Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children. Consider the camera angle; photographs taken over the shoulder, or from behind are less identifiable.
- Use images of children in suitable dress, and take care when photographing PE or swimming events to maintain modesty.
- Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.
- Children can be identified by logos or emblems on sweatshirts etc. Depending on the use to which the photograph will be put, consider airbrushing logos.
- Consider alternatives. Is a photograph of the children necessary, or could an article be illustrated by the children's work for example.

General guidelines for staff using digital images of children and young people can be found in Appendix A 3.

3. Identifying children and young people

Good practice with regards to the identification of children and young people when using digital media suggests that:

• If the pupil is named, avoid using their photograph
• If the photograph is used, avoid naming the pupil.

It is suggested that:

• the minimum amount of information is used. Is it really necessary to accompany a picture with the pupils' names, the year group, or the school?
• When ***fully*** naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

4. Using photographs of children supplied by a third party

Copyright **does not** apply to images for **private family** use.

However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it.

If you commission photographs for use at school make sure that you include in the contract that the school will own the copyright for items taken on your behalf.

Before using a photograph supplied by a third party you should check that the third party owns the copyright in the photograph and you should obtain their written or verbally recorded permission to use it.

f you use a photograph without the copyright owner's permission you could find that an action is taken against you for copyright infringement.

Images downloaded from the Internet are also subject to copyright. Do not use sources like Google images to find photographs use a reputable stock images website or take advice.

Third Parties will generally be under the same obligations as your school to obtain parental consent to the use and distribution of photographs. You should therefore ask the third party to guarantee to you that all relevant consents have been given and that they are entitled to provide you with the image.

5. Use of Images of children by the Press

(Please refer to the recommendations in section 3 above; 'Identifying Pupils')

There may be occasions where the press take photographs at your school of pupils. The consent form identified in Appendix B attempts to highlight the potential risks for parents so that they can make an informed decision about whether to agree to their children being featured in the press and whether their full name should accompany the photograph.

The manner in which the press use images is controlled through relevant industry codes of practice as well as the law. However, given your responsibility to parents and pupils, it is sensible to politely check that broadcasters and press photographers you may be chaperoning on your school premises are aware of the sensitivity involved in detailed captioning, one to one interviews, and close or sports photography.

6. School Prospectuses and other literature

Although most school literature is sent to a specific audience, it would be best to avoid using personal details or full names of any child in a photograph. See the advice given in sections 2, 3 and4 of this document.

7. Videos

You must have parental consent before any child can appear in a video, Parents can make video recordings of nativity plays and other such events for their own personal and family use, as they are

not covered by the Data Protection Act (cross reference with section 10 of this document).

Potential difficulties in this area could be avoided if the school adopts the policy of taking an official video of the event and making copies available to parents.

8. Websites

Web use can be of particular concern to parents and staff because of the potential misuse of images. With digital photography there is the remote possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge.

The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on websites can be made more difficult to copy by several measures such as:

• copy-protection,
• overlaying with a watermark,
• publishing in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website. Increasingly, users are generating content for websites e.g. children, young people and adults placing pictures on social networking web sites. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites.

Itis essential that schools have an e--safety policy and acceptable use guidelines.

9. Webcams

The regulations for using webcams are similar to those for CCTV (closed-circuit television). This means that the area in which you are using the webcam must be well signposted and people must know that the webcam is there before they enter the area, in order to consent to being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all the affected children.

In gaining consent, you must tell the person why the webcam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access.

There are both benefits &risks to the use of webcams and good practice suggests that unless a webcam is a response to a specific threat or difficulty in relation to either crime or health and safety it may pose more difficulties for the school than it would actually resolve. If you want to use a webcam, it would be prudent to undertake careful parental, staff, and legal consultation.

10. Parental right to take photographs

Parents are not covered by the Data Protection Act 1998 if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays.

Parents are **not** permitted, however, to take photographs or to make a video recordings for anything **other than their own personal use** (e.g. with a view to selling videos of a school event).

Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the Data Protection Act 1998 would be breached. The consent form included in Appendix B and guidance for parents and carers outlined in "Use your camera and video courteously" in Appendix C reminds parents of this fact.

When hosting an event where parents are permitted to take photographs or DVD footage, make it clear from the start that any images taken must be for private use only and ask for them not to be put on the web otherwise Data Protection legislation may be contravened. You might want to consider putting this in writing to parents/carers prior to the event (see Appendix C for example) and/or make an announcement at the start of the event.

Data Protection considerations aside, it is possible to consider banning all filming / recording / photography of school productions, sports days etc. if you feel that this is appropriate. Many parents would consider it to be over--cautious to impose such a ban and due consideration must be given on this course of action. Should you wish to impose any such ban we would advise you to take legal advice in order to ensure that the correct steps are taken, whilst acknowledging that such a ban would be difficult to enforce.

The important thing is to be sure that people with no connection with your school do not have any opportunity to film covertly. Ask your staff to quiz anyone they do not recognise who is using a camera or video recorder at events and productions and include this instruction in your consent form or any event tickets.

11. The storage of photographs

Photographs must be maintained securely for authorised school use only and disposed of either by return to the child, parents, or shredding as appropriate in line with record retention schedules.

Storage should include reference to the permissions obtained and their currency and staff should be aware that images should not be removed from institutional computers and taken home.

If permission is withdrawn for a photograph it must be edited from the storage immediately.

12. Official School Photographs

Schools will periodically invite an official photographer into school to take portraits/photographs of individual children and/or class groups. It is essential that when considering such an activity, schools undertake their own risk assessment in terms of the validity of the photographer/agency involved and establish what checks/vetting has been undertaken (e.g. CRB). Procedures should also ensure that levels of supervision are appropriate to safeguard the welfare of children at all times when visitors are present on the school site.

13. Images taken by young people

Schools will have their own policies on use of mobile phones, camera phones and digital cameras by children and young people. Where such equipment is allowed it is important that schools have policies and codes of conduct for safe usage and advice on inappropriate usage and possible consequences of misuse.

Areas of increased concern would involve residential trips and usage in bedrooms, swimming. Children and young people may need to be made aware that taking and distributing inappropriate photographs may be a criminal offence.

14.Useful sources of information

DfE Guidance for schools on the use of photographs and video images of children for publicity purposes:
http://www.education.gov.uk/schools/pupilsupport/pastoralcare/childprotection/policy/a0010833/child-protection-guidance-for-schools-on-the-use-of-photographs-and-video-images-of-children-for-publicity-purposes

DfE Guidance for schools on photographic images and the press:
http://www.education.gov.uk/schools/pupilsupport/pastoralcare/childprotection/policy/guidance/a0010835/child-protection-guidance-for-schools-on-photographic-images-and-the-press

Child Exploitation and On--line Protection centre www.ceop.gov.uk

Think you know --www.thinkyouknow.co.uk/

The Information Commission website at www.dataprotection.gov.uk

Press Complaints Commission Code of Practice at www.pcc.org.uk

This guidance is produced with thanks to Kent County Council for the original document.

Appendix A

Guidance for Staff Using Digital Images of Children and Young People

It is a requirement that, when using a photograph or photographic equipment, the following guidelines must be followed:

- Ensure that you have the appropriate consent when planning to use digital images of children and young people as detailed in the school's "Use of photographic Images" policy.
- Ensure that a member of the senior management team is aware that you will be using the school's photographic/video equipment is being used and for what purpose. Make sure that you sign the equipment in and out to account for the use of equipment.
- Staff must not use their personal photographic/video equipment, nor take images of children and young people using personal mobile telephones under any circumstances
- Staff should remain sensitive to any children who appear uncomfortable and should recognise the potential for misinterpretation. Avoid taking images in one-to-one situations. Do not use images that are likely to cause distress, upset or embarrassment
- A member of staff should establish whether the image(s) will be retained for further use. Images should be securely stored on a school computer or data card and used only by those authorised to do so.
- Staff should ensure that all images are available for scrutiny and be able to justify images of children in their possession.
- Staff should report any concerns relating to any inappropriate or intrusive photography to a member of the senior management team.
- If any resulting digital image is used, avoid naming the pupil.
- If the pupil is named, avoid using a digital image.
- Ensure all children are appropriately dressed.
- Avoid images that show a single child with no surrounding context of what they are learning or doing. A group of three or four children is more likely to show the activity to better effect. Use photographs that represent the diversity of the young people participating.
- Be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded.
- It is not appropriate to take photographs of a pupil's injuries, whether they are accidental or non-accidental, as it may cause distress and humiliation. If appropriate, seek medical help and in the case of a suspected non-accidental injury contact the Designated Senior Person for Child Protection immediately.

Appendix B
Consent form for the use of images of children

To:

Name of child:
School:

Occasionally, we may take photographs of the children. We may use these images in our publicity or the schools/setting prospectus or in other printed publications as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

From time to time, our establishment/school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, websites or on televised news programmes.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer questions 1 to 5below, then sign and date the form where shown.

If your child is old enough to express their own view, you may want to consult with them about the categories of consent, and we invite you to use this letter to explore their feelings about being photographed at school.

PLEASE RETURN THE COMPLETED FORM TO THE SCHOOL AS SOON AS POSSIBLE.

Please circle your answer

1. May we use your child's photograph (unidentified) in the school prospectus and other printed publications that we produce for promotional purposes?	Yes/No
2. May we use your child's image (unidentified) on our website?	Yes/No
3. May we record your child's image (unidentified) on video or webcam?	Yes/No
4. Do you consent to your child being photographed or filmed in press events agreed by the school?	Yes/No
5. Do you consent to your child's full name being published with a press photograph?	Yes/No

*****Please see notes at end of document *****

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies. "Unidentified" above means we will only use the first name. Please also note that the conditions for use of these photographs are on the back of this form.

I have read and understood the conditions of use on the back of this form.

Parent's or guardian's signature: Date:

Name (in block capitals):

Conditions of school use

1. This form is valid for five years from the date you sign it, or for the period of time your child attends this school or setting. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your agreement in writing at any time.

2. We, the school, setting or service, will not use the personal details or full names (which means first name and surname) of any child in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.

3. We will not include personal e--mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

4. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption, unless we have your agreement.

5. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

6. We may include pictures of pupils and teachers that have been drawn by the pupils.

7. We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”.

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

9. **As the child’s parents/guardian, we agree that if we take photographs or video recordings of our child/ren which include other pupils, we will use these for personal and family use only.** I/we understand that where consent has not been obtained from the other parents for any other use, we would be in breach of the Data Protection Act 1998 if we used our recordings for any wider purpose.

Appendix C

'Use your camera and video courteously'

A guide for parents who wish to use photography and/or video a school event

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves. By following some simple guidelines we can proceed safely and with regard to the law.

- Remember that parents/carers and others, attend school events at the invitation of the head and governors

- The head and governors have the responsibility to decide if photography and videoing of school performances is permitted

- The head and governors have the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.

- Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos must not be sold and must not be put on the web/internet. To do so would break Data Protection legislation.

- Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.

- Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

- Parents and carers must not photograph or video children changing for performances or events

- If you are accompanied or represented by people that school staff do not recognise they may need to check who they are, particularly if they are using a camera or video recorder. v. Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.

Appendix 12 – Photography Permission Form

ST MICHAEL'S
Church of England High School

Photograph Permission Form

Name of Student	
Form	

This form must be returned to Form Tutors as soon as possible.

I agree to my child's photograph/video to be used in the following ways:	
• School Prospectus	☐
• Curriculum document	☐
• *School website	☐
• *School social media	☐
• *LA website	☐
• LA material	☐
• School displays aimed at the school community	☐
• Displays within school or external exhibitions	☐
• Media coverage within the school	☐
• As an example of good practice and training materials	☐
	(please tick as appropriate)

* Please note that internet websites can be viewed worldwide

Please note: student photographs are also used on our Management Information System which is only accessed by staff.

Names are normally disclosed to celebrate an event, e.g., newspaper coverage.

Data Protection Act1988: The school is registered under the Data Protection Act for holding personal data. The school has a duty to protect this information and to keep it up to date. The school is required to share some of the data with the Local Authority and with the DfE.

Signature: _____ Date: _____

Name:_____ Date:_____
(please print)

Appendix 13 - Privacy Notice

ST MICHAEL'S
Church of England High School

Fair Processing Statement

Date of approval	May 2016
Review date	May 2018

Privacy Notice – Data Protection Act1998

We, St Michael's Church of England High School, are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- support your learning;
- monitor and report on your progress;
- provide appropriate pastoral care; and
- assess how well we are doing.

Information about you that we hold includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications the Learning Records Service will give us your unique learner number (ULN) and may also give us details about your learning and qualifications.

In addition for secondary aged pupils

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority (LA) support service for young people aged 13 to 19 in England. We must provide the names and addresses of you and your parent(s) and any further information relevant to the support services role.

However, if you are 16, you (or your parent(s)) can ask that no information beyond names, addresses and your date of birth be passed to the support services. This right transfers to you on your 16th birthday. Please tell the Data Manager if you wish to opt out of this arrangement. For more information about young people's services go to the National Careers Service page at https://nationalcareersservice.direct.gov.uk/aboutus/pages/default.aspx

Section 72 of the Education and Skills Act 2008 requires all schools to provide relevant information about pupils to LA that helps to identify those at risk of ending up not in education, employment or training (NEET) post 16.

Triple S

"The results of physical tests for individual children, e.g. a test of a child's balance, carried out as part of the Triple S programme may be passed to the LA. Pupils are able to opt out of both the physical tests and the recording of height and weight as part of the Triple S program. These results may be matched to other data held by the LA on these children and used for the production of school and group level statistics. It will not be possible to identify individual pupils from the statistics.

We will not give information about you to anyone outside the school without your consent unless the law and our policies allow us to.

We are required by law to pass some information about you to our LA and the Department for Education (DfE).
If you want to see a copy of the information about you that we hold or share, please contact the

Data Manager.

If you require more information about how the LA and DfE store and use your information, then please go to the following websites:

Sandwell Council website - Privacy Notice

How the Department for Education shares pupil and workforce data

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Data Protection Officer
Sandwell Council House
PO Box 16230
Oldbury
West Midlands
B69 9EX

Ministerial and Public Communications Division
Department for Education
Piccadilly Gate
Store Street
Manchester
M1 2WD

Website:	https://www.gov.uk/government/organisations/department-for-education
Contact:	https://www.gov.uk/contact-dfe
Telephone:	0370 000 2288
	Monday to Friday, 9am to 5pm

Appendix 14 – IT Policy – Staff

ST MICHAEL'S
Church of England High School

IT Policy

Date adopted	18th October 2017
Next revision date	October 2019

Headteacher: **Mrs J Gray, MSc, NPQH**

St Michael's Church of England High School • Rowley Learning Campus • Curral Road • Rowley Regis • West Midlands • B65 9AN
Telephone: **0121 561 6881** • Fax: 0121 561 6882 • email: contact.staff@st-michaels.sandwell.sch.uk

Contents:

Appendices

Statement of intent

St Michael's Church of England High School believes that IT plays an important part in both teaching and learning over a range of subjects.

The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

This policy covers the rules and procedures for authorised and unauthorised use of the IT and communication facilities and is implemented in conjunction with the school's E-safety Policy.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

1. Overview

1.1. The IT facilities at St Michael's Church of England High School are defined as:

- Computers and software
- Monitors
- Keyboards
- Computer Mice
- Printers
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- The communication facilities at St Michael's Church of England High School are defined as:
    - Telephones
    - Fax machines
    - Televisions
    - Video players
    - DVD players
    - Satellite receivers
    - Mobile phones
    - Projectors
    - Display screens
    - Other devices including fittings used with them
    - Internet and e-mail can be defined as a communication facility used in conjunction with IT facilities; as such, these will coincide with the IT facilities.

1.2. This policy contains:

- The school's view on the use of e-mail and the internet at work.
- An explanation on what you can or cannot do.
- The consequences if you fail to follow the rules set out in this policy.
- General information relating to IT, including the Data Protection Act.
- How the policy is implemented.
- The Managed Service Provider's duties to the IT policy.

2. Policy

2.1. The use of the IT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency.

2.2. Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, can cause many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

2.3. Staff should always be an example of good practice to the students, serving as a positive role model in every aspect.

2.4. Abuse of the IT facilities could result in the facilities being removed. Staff should always be aware of IT use, and misuse of the facilities, as defined in this policy, must be reported to the Headteacher.

2.5. Students are bound by the Acceptable Use Policy.

2.6. Staff should make sure that pupils comply with that policy.

2.7. Students misusing the IT facilities must be reported to the Headteacher.

2.8. This policy applies to any computer connected to the school's network and computers.

2.9. Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

2.10. A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

3. Procedure

3.1. The school's e-mail system and internet connection are available for communication and use on matters directly concerned with school business.

3.2. Employees using the school's e-mail system and internet connection should give particular attention to the following points in this policy.

3.3. E-mail should not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

3.4. "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships.

3.5. Hasty messages, sent without proper consideration, can cause unnecessary misunderstanding.

3.6. If an e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.

3.7. The school will be liable for any defamatory information circulated either within the school or to external contacts.

3.8. The school's e-mail system and accounts must never be registered or subscribed to unsolicited e-mail (SPAM).

3.9. Never disclose any of the school's e-mail addresses without confirming that they will not be subjected to SPAM and that they will not be sold on to marketing companies.

3.10. All e-mails that are sent or received must be retained within the school for a period of six months.

3.11. All e-mails being sent to external recipients must contain the school's address and the direct contact details of the sender.

3.12. Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect the IT facilities. If unsure, seek assistance or approval from the Managed Service Provider.

3.13. Offers or contracts sent via e-mail or the internet are as legally binding as those sent on paper. An exchange of e-mails can lead to a contract being formed between the sender, or the school, and the recipient. Never commit the school to any obligations by e-mail or the internet without ensuring that you have the authority to do so. If you have any concerns, contact the Headteacher.

3.14. Online purchases are only permitted with the Headteacher present, in order to comply with monitoring and accountability. Hard copies of the purchase must be made, for the purchaser and the Business Manager - Finance. This is in addition to any purchasing arrangement followed according to school policy.

3.15. Any failure to follow these procedures satisfactorily may result in disciplinary action, including summary dismissal.

4. Authorised use of the IT facilities

4.1. The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Personal e-mail accounts are only permitted to be used if they have built-in anti-virus protection approved by the Managed Service Provider. Access to your personal e-mail must never interfere with your work duties.

5. Authorised use of the communications facilities

5.1. The communication facilities should only be used as required by your work duties. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any school encouraged tuition or educational use

5.2. If unsure about your required use, please seek authorisation from the **Headteacher**.

6. Unauthorised use of the IT facilities

6.1. It is not permitted under any circumstance to:

- Use the IT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage the IT facilities.
- Re-locate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the Assistant Headteacher Facilities and Resources or Headteacher. Certain items are asset registered and security marked; their location is recorded by the financial assistant for accountability. Once items are moved after authorisation, staff have a responsibility to notify the financial assistant of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone. This is illegal under the Computer Misuse Act.

6.2. Use the IT facilities at any time to access, download, send, receive, view or display any of the following:

- Any material that is illegal
- Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- Online gambling
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit content

6.3. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.

6.4. Install hardware or software without the consent of the Assistant Headteacher Facilities and Resources, the Managed Service Provider or the Headteacher.

6.5. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act.

6.6. Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.

6.7. Purchase any IT facilities without the consent of the Assistant Headteacher Facilities and Resources or the Headteacher. This is in addition to any purchasing arrangements followed according to school policy.

6.8. Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.

6.9. Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, you must not download or attempt to download any software.

6.10. Use the internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher. This is in addition to any purchasing arrangement followed according to school policy.

6.11. Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.

6.12. Use the IT facilities for personal use without the authorisation of the Headteacher. This authorisation must be requested on each occasion of personal use.

6.13. Copy, download or distribute any material from the internet or e-mail that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.

6.14. To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.

6.15. Interfere with someone else's use of the IT facilities.

6.16. Be wasteful of IT resources, particularly printer ink, toner and paper.

6.17. Use the IT facilities when it will interfere with your responsibilities to supervise students.

6.18. Any unauthorised use of e-mail or the internet is likely to result in disciplinary action including summary dismissal.

6.19. If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately to your line senior or the Headteacher.

7. Unauthorised use of the communications facilities

7.1. It is not permitted under any circumstance to:

- Use the communication facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage the communication facilities.
- Use the communication facilities for personal use without authorisation from the Headteacher with the exception of the circumstance in 7.2.
- Re-locate, take off-site or otherwise interfere with the communication facilities without the authorisation of the Headteacher.

7.2. Use the communication facilities at any time to access, receive, view or display any of the following:

- Any material that is illegal
- Any material that could constitute bullying, harassment (including on the grounds of sex, race religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit material
- Any adult or chat-line phone numbers
- Use or attempt to use the school's communication facilities to undertake any form of piracy, including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.
- Use or attempt to use the school's communication facilities for internet or e-mail access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.
- Copy, record or distribute any material from or with the communication facilities that may be illegal. This can include television media, films, telephone conversations and music. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- Use or attempt to use the communication facilities to call overseas without the authorisation of the Headteacher.
- Use the communication facilities when it will interfere with your responsibilities to supervise students.
- Use of the school's telephone facilities for personal use is permitted for necessary calls lasting less than 10 minutes. Should you need to use the telephones for longer than this, then authorisation must be sought from the Headteacher. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls. However, the duty head or Headteacher must be notified after the call. Any personal use of the telephones may be subject to a charge; this is at the Headteacher's discretion.

7.3. All items are asset registered and security marked, their location is recorded by the financial assistant for accountability. Once items are moved following authorisation, staff have a responsibility to notify the financial assistant of their new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

7.4. If you are subjected to or know about harassment or bullying, you are encouraged to report to your line senior or Headteacher.

8. Implementation of the policy

8.1. Staff are requested to report any breach of this policy to the Headteacher.

8.2. Regular monitoring and recording of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages can be used as evidence in disciplinary proceedings.

8.3. Use of the telephone system is logged and monitored.

8.4. Use of the school's internet connection is recorded and monitored.

8.5. The financial assistant randomly checks asset registered and security marked items.

8.6. The Managed Service Provider checks computer logs on the school's network regularly.

8.7. Unsuccessful and successful log-ons are logged on every computer connected to the school's network.

8.8. Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

8.9. The Managed Service Provider can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement the IT Policy and to assist in any difficulties.

8.10. The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.

8.11. The school's database systems are computerised. Unless your line manager gives you express permission, you must not access the system. Failure to adhere to this requirement may result in disciplinary action.

8.12. All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. Do not, under any circumstances, disclose this password to any other person.

8.13. Attempting to access the database using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

8.14. User accounts are accessible by the Headteacher and the Managed Service Provider.

8.15. Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

8.16. Users are required to be familiar with the requirements of the Data Protection Act 1998 and, from 25th May 2018, the General Data Protection Regulation and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but employees must adhere to the following rules:

- Do not disclose any material about a person, including a pupil, without their permission
- Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences
- Do not send any personal data outside the UK

9. Storing messages

9.1. Messages should be deleted after six months or stored in a suitable hard copy file.

9.2. Information and data on the school's network and computers should be kept in an organised manner and should be placed in a location of an appropriate security level.

9.3. If unsure, please seek help and information from the Assistant Headteacher Facilities and Resources and/or the Managed Service Provider.

9.4. Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their line manager or Headteacher, as appropriate. The complaint can then be raised through the grievance procedure.

10. The Third Party IT Managed Service Provider duties

10.1. To monitor and affect accountability of the IT policy, the Managed Service Provider is required to:

- Carry out daily checks on internet activity of all user accounts and to report any inappropriate use to the Headteacher.
- Monitor the computer logs on the school's network and to report any logged inappropriate use to the Headteacher.
- Remotely view or interact with any of the computers on the school's network. This may be done randomly to implement the IT policy and to assist in any difficulties.
- Access files and data to solve problems for a user, with their authorisation. If an investigation is requested by the Headteacher, authorisation from the user is not required.
- Adjust access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disable user accounts of staff that do not follow the policy, at the request of the Headteacher.
- Assist the Headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to the IT Policy.
- Assist staff with authorised use of the IT facilities, if required.

11. Policy review

11.1. This policy is reviewed every two years by the Assistant Headteacher – Facilities and Resources and the Headteacher.

11.2. The scheduled review date for this policy is October 2018.

Appendix 1: Technology acceptable use agreement

Name of school: St Michael's Church of England High School

Date:

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly, and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other pupils, staff or third parties.
- I will ensure that any personal data is stored in line with the Data Protection Act 1998.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the data protection officer or headteacher.
- I will only use recommended removable media, and will keep this securely stored.

- I will provide removable media to the data protection officer for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the Headteacher or Assistant Headteacher, Facilities and Resources.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents.
- I will ensure that any school data stored on school or personal mobile devices is password protected, and give permission for the Assistant Headteacher, Facilities and Resources to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over social networking sites.
- I will ensure that I apply the necessary privacy settings to my social networking sites.
- I will not publish any comments or posts about the school on my social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Assistant Headteacher, Facilities and Resources to undertake regular audits in order to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

5. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the **E-Safety Policy**, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the Headteacher.
- I understand that my use of the internet will be monitored by the Assistant Headteacher, Facilities and Resources and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Allegations Against Staff Policy, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed: _____ Date:_____

Staff Member

Print name:_____

Signed: _____ Date:_____

Headteacher

Print name:_____