Date ratified at Directors Meeting 14 July 2016	Review Date Directors May 2017

St John the Baptist Catholic Multi Academy Trust

THE MAT MISSION STATEMENT

Our family of schools is united in the belief that God's love, peace, truth, and joy is for all. We are dedicated to the achievement of excellence in all we do. We cherish the uniqueness of each of our school communities and celebrate together as one Trust family. By following Jesus' example we bear witness to the greatness of God.

'To think, to feel, to do' *Pope Francis*

St John the Baptist Catholic MAT
Company No: 7913261
Registered Office: Surrey Street, Norwich NR1 3PB

Acceptable Use Policy
(including the Online safety policy)

IN TRAN communication for all

If you need this document in large print, audio, Braille, alternative format or in a different language please contact the Company Secretary on 01603 611431 and we will do our best to help

Contents

1. Preamble

St John the Baptist CMAT recognises that IT and the Internet are tools for learning and communication that can be used in each school to enhance the curriculum, challenge students, and support creativity and independence.

At St John the Baptist CMAT we provide pupils with a broad and balanced curriculum that promotes the spiritual, moral, social and cultural (SMSC) development of our pupils.

Pupils will be encouraged to regard people of all faiths, genders, races and cultures with respect and tolerance.

All users are bound by the SJB CMAT ethos of mutual-respect.

Our guiding principle is in the education of our community *about* ***User Responsibility*** as this enables:

- ***the educational use*** of the new e-technologies available;
- ***the respectful use*** of e-technologies with regard to the MAT's ethos and the *fundamental British values*, including *democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths; beliefs* together with gender;
- ***the safe use*** of e-technologies so that all users are kept safe from harm

Using IT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and IT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm others. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children. Educating all members of the school community on the responsibilities and risks of online safety falls under this duty.

It is important that there is a balance between controlling access to the internet and e-technologies and allowing freedom to explore and use these tools to their full potential.

This policy aims to be an aid in regulating IT activity in school, and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online outside of school hours.

Cyber bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in the local school **Behaviour for Learning Policy** and **Anti-Bullying policy,** where the school has one**.**

Finally, the Computer Misuse Act 1990 identifies three specific offences:

1. Unauthorised access to computer material (that is, a program or data).
2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
3. Unauthorised modification of computer material

If the Computer Misuse Act 1990 is breached then a student or member of staff is likely to have the matter referred to other authorities including the police.

Online safety is a whole-school issue and responsibility. Please refer to other relevant policies, i.e. policies covering Data Security, Use of CCTV etc.

2. Roles and Responsibilities

2.1 Directors and Local Governing Bodies

The Directors are responsible for the approval of the Acceptable Use Policy and for reviewing the effectiveness of the policy by reviewing online safety provision. The implementation of the policy is delegated to the LGBs. Online safety falls within the remit of the Local Governor responsible for Safeguarding.

The role of the Directors and Local Governors will include:

- To ensure an Acceptable Use Policy incorporating Online safety is in place, reviewed annually and is available to all stakeholders.
- The policy may be reviewed more frequently if significant changes occur with technologies in use in the schools. The online safety policy is referenced within other school policies e.g. the Safeguarding and Child Protection Policy.
- To ensure that procedures for the safe use of IT and the Internet are in place and adhered to.
- To receive and challenge the annual online safety audit toward improvements, referring to the Critical Security Control checklist (NCC Online Safety Policy February 16 – see Appendix 10.)
- To hold the Headteacher and staff accountable for Acceptable Use / Online safety practice.

2.2 Senior Designated IT Lead (SDITL)

The Senior Designated IT Lead will be a role delegated to a member of the Leadership Team in each school reporting to the Headteacher who has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online safety Co-ordinator. In small schools the Headteacher can also be the SDITL.

Any complaint about staff misuse must be referred to the SDITL at the school or, in the case of a serious complaint, to the Headteacher.

The SDITL will:

- Ensure that there is an Online safety Coordinator who has received appropriate CEOP training.
- Ensure access to induction and training in Online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a member of LT or equivalent.
- Ensure that pupil or staff personal data as recorded within the school management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and school IT Manager

(or equivalent) to ensure systems to protect students are reviewed and improved.

- Ensure the school IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Ensure that the relevant Governors sub-committee will receive monitoring reports from the Online safety Co-ordinator on a termly basis.

2.3 IT Services Manager / IT Technicians

In addition to their job description the IT Services Manager or IT Technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body's Online safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, the internet, the Virtual Learning Environment, remote access, and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or Online safety Coordinator for investigation, action, sanction or support.
- That monitoring software / systems are implemented and updated as agreed in school policies.

2.4 The IT Steering Group (or relevant Governors sub-committee which considers IT & e safety)

- This group of staff will advise, oversee and support the provision of Acceptable Use and online safety in the particular school within the St John the Baptist CMAT.
- The school will audit IT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate and effective.

2.5 Communicating School & MAT Policy

This policy is available *on the MAT website* for parents, staff, and pupils to access as and when they wish.

Rules relating to the school code of conduct when online, and online safety guidelines, are to be displayed around the school.

Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, for example during PSHE lessons and as part of the Computing curriculum, where personal safety, responsibility, and/or development are being discussed. In the Primary phases, discrete lessons are based on the materials provided by CEOP.

Staff who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues**.**

2.7 Authorising IT access

All users must read, acknowledge and accept the '**Acceptable User Agreement' annually** before using any school IT resource. E.g. through the use of a pop-up to acknowledge prior to resuming use of their IT account. This is part of the terms and conditions of working within St John the Baptist CMAT.

Each school will maintain a current record of all staff and pupils who are granted access to school IT systems.

If a school account is dormant for two weeks during term-time, it may be suspended temporarily.

3. Managing IT Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats.

The IT Manager or IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly.

Any internet resources that staff sign up to for school purposes must be done using a school email account.

Students must not be granted access to any school or online resources via personal email accounts

Some safeguards that the school takes to secure our computer systems are:-

- Working toward a system to ensure that all personal data sent over the Internet is secure e.g. encrypted.
- Working toward a system so that staff are fully aware of their responsibility for ensuring that all personal data taken off site is secure.
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this.
- Files held on the school network will be regularly checked for viruses.
- The use of user logins and passwords to access the school network will be mandatory.

- Portable media containing school data or programmes will not be taken off-site unless encrypted or password protected.
- The SIDT leader will support staff with choosing and using suitable passwords and help with other online safety/computer use queries.

4. Online safety Curriculum

4.1 Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Pupils should be taught what internet use is acceptable and what is not and given clear objectives for Internet use as part of the curriculum. Assemblies and also class time may be used to support this.

Pupils should be educated in the effective use of the internet by their class teachers as appropriate and in discrete Computing lessons e.g. which sites to access; how to use the internet to research; not to copy and paste large chunks of the internet, how to use the CEOP Report abuse button etc.

Pupils will be shown how to publish and present information appropriately to a wider audience, as part of their curriculum, and as appropriate to their courses.

Online safety rules will be posted in all networked rooms including the Library.

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. The pupils should be taught that visiting any websites and communicating online leaves a 'digital footprint'.

All users are to be aware that Internet traffic can be monitored and traced to the individual user. Discretion and appropriate conduct is essential.

Pupils should be taught to:

- Be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be sanctioned. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

- use age-appropriate tools to search for information online

- how and why to report inappropriate conduct online / unpleasant Internet content e.g. using the CEOP Report Abuse icon

Pupils will be informed that emails, network and Internet use will be monitored.

4.3 Managing filtering

The School will set the guidance on the use of filtering. The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *school online safety coordinator.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or any consequences of internet access.

The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

The school will consider requests for access to key sites on a case by case basis.

The school will work in partnership with Norfolk and Suffolk Children's Services to ensure systems to protect pupils are reviewed and improved.

For more information on data protection in school and across the MAT, please refer to our **Data Protection Policy**.

More information on protecting personal data can be found in **Section** 9 of this policy.

4.4 Parents' support

Parents' and carers' attention will be drawn to the Online safety Policy on enrolment of their child, in newsletters, the school brochure and on the school web site.

Parents and carers will from time to time be provided with additional information about online E-safety.

Acceptance of a place at a school within the MAT and subsequent enrolment confirms the agreement of parents and students to support and abide by all school policies and procedures in place and as varied from time to time.

4.5 Handling Online safety complaints

Any complaint about staff misuse must be referred to the SDITL at the school or, in the case of a serious complaint, to the Headteacher. If the complaint is about misuse by the Headteacher, it must be referred to the Chair of Governors.

Complaints of Internet misuse by students will be dealt with:

- at primary phase – by the appointed member of the school Leadership Team
- at secondary phase – by the pastoral leader for that student, e.g. a Head of Year or Class teacher in conjunction with other staff as appropriate e.g. safeguarding team; E-safety coordinator.

Concerns of a Safeguarding nature must be referred to the Designated Safeguarding Lead and their team and dealt with in accordance with school procedures.

5. Cyber bullying

The school, as with any other form of bullying, takes Cyber bullying seriously. Information about specific strategies to prevent and tackle bullying is set out in the **Behaviour for learning policy** and the **Anti-Bullying policy.**

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

If an allegation of bullying involving the use of IT or any emerging technology does take place, the school will:

- Follow the policy and procedures for dealing with bullying
- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the person causing concern.
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the person causing concern that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the person causing concern will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

6. Use of Email

It is important that users of our email systems should be confident about the following:

- The identity of the user of the email account with whom they are communicating.
- The security of the communications and any data sent.
- That the school has access to an audit trail of the conversation in the event of any issues arising.

6.1 Staff Use of Email

Staff school email accounts should be used for any and all school business and most especially when communicating with students, parents and external organisations and individuals on school business.

Be aware that emails have legal force i.e. what you say in an email has as much legal standing as something you write on paper.

Personal email accounts should not be used in a professional capacity.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

The forwarding of chain messages is not permitted in school.

6.2 Email Communication with Students

Staff must only have email contact with students using their school accounts.

Students must use only their school email accounts to contact staff.

If a student emails from a personal email address staff may reply but only to ask them to use their school email address for communication.

People not employed by the school but communicating with students for school purposes must use a verifiable business email account not a personal email account. If they do not have one then the school will provide one.

6.3 Student email

Students may only use approved e-mail accounts on the school system.

Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone unknown.

Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school will monitor how e-mail from pupils to external bodies is presented and controlled:

- primary phase – all emails going to an outside agency or person, must be checked by a teacher first
- secondary phase - students should copy in the supervising teacher.

Pupils will be educated through the IT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

6.4 Email communication with parents

Email communication with parents should occur only to the email address registered to them in the school MIS.

Confidential information must ***not*** be sent by email to parents as our emails are not encrypted.

6.5 Internet Resources

Internet resources that users sign up for school purposes must be done using a school email account.

Students must not be granted access to any resources using any form of personal email accounts.

7. The School Website

The contact details on the website should be the school address, e-mail and telephone number.

Staff or pupils' personal information will not be published.

7.1 Published Content

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published.

For information on school policy on children's photographs published on the school website please refer to section 9 of this policy.

8. Social networking

The school will control access to social networking sites, and will educate pupils in their safe use e.g. use of passwords.

All students will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

Pupils must not place personal photos on any social network space provided in the school IT resources without permission.

Pupils, parents and staff will be advised on the safe use of social network spaces.

Pupils will be advised to use nicknames and avatars when using social networking sites.

8.1 Social Media, Social Networking and Personal Publishing on School IT resources

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. *There are various restrictions on the use of these sites in school that apply to both students and staff.*

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through curriculum areas such as IT and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites (including gaming sites) and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of IT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Official school blogs created by staff / students for the school IT resources are not to be publicly visible unless approved by the IT Steering Group or relevant Governors sub committee. They will be moderated by a designated member of staff.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction.

9. Data

9.1 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

The school will follow these principles of good practice when processing data:

- Ensure that data is fairly and lawfully processed

- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the MAT & school's safeguards relating to data protection read the **Data Protection Policy.**

9.1.1 File sharing services e.g. Google
With any service that shares files e.g. Google, do not "share" any files unless you are confident about how the system works, and who will be able to access the data.

Key Example
For example, all school-related Google material must at every stage be created and worked on via the school Google account (not a private account). This is partly because shared files originating "at home" will carry the home account email on them, even after "sending" them to school. This is different to more unified systems such as Microsoft.

9.2 Images

Colour photographs and pupils' work bring our school to life, showcase our students' talents, and add interest to publications both online and in print. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have safeguards in place.

It is important that published images do not identify students or put them at risk of being identified.

Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

The school follows general rules on the use of photographs of individual children:

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect the use to which you are consenting. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- For how long parents are consenting the use of the images
- School policy on the storage and deletion of photographs.

On admission, parents or carers will complete a consent form to give permission from parents or carers before names, photographs or images of pupils are published.

A template of the consent form can be found at the end of this policy.

Photographs that include pupils will be selected carefully and the school will look to seek to use group photographs rather than full-face photos of individual children.

Pupils' full names will be avoided on publicly accessible school IT resources as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Staff and external parties will be made aware of the restrictions on photographing certain students through the website and relevant policies.

9.3 Complaints of Misuse of Photographs or Video

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

9.4 Use of photography and filming at school events.

All schools in the MAT will follow the NCC guidance for schools – 'Guidance for schools: Parents and Carers use of photography and filming at school events. See Appendix 11.

10. Mobile Phones and Personal devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are they:

- can make pupils and staff more vulnerable to cyber bullying
- can be used to access inappropriate internet material
- can be a distraction in the classroom
- are valuable items that could be stolen, damaged, or lost
- can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school.

At primary phase:

- Parents must write to the school, explaining why the child needs their mobile phone in school and the school will store the phones during the school day. Children must hand these in at the start of every school day and they can then be collected at the end of the school day through the individual school's system. Should a child knowingly not hand their phone in at the start of the school day, this issue will be managed through the school's Behaviour Management policy.

At secondary phase:

- Mobile phones and associated cameras will not be used during lessons except as part of an educational activity.

    - The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy.**
    - Mobile phones must be switched off during school lessons or any other formal school activities.
    - Images or files should not be sent between mobile phones in school.
    - A member of staff can confiscate mobile phones if used inappropriately.
    - A member of the leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
    - Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
    - If staff wish to use these devices in class as part of a learning project, they must follow the above guidance

Staff should not share personal telephone numbers with pupils and parents. A school phone will be provided for staff where contact with pupils is required.

Pupils

- Pupils who breach school policy relating to the use of personal devices will be sanctioned in line with the school's behaviour policy. Their mobile phone may be confiscated.

- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- In nurseries, staff are not permitted to bring their mobile phones into areas used by children. Personal belongings, including mobile phones, should always be stored in the nursery office.
- Staff should not use their personal mobile phones to contact pupils or parents either in or out of school time for any school-related purpose. The only exception would be in an emergency and it would need to be logged with the Office staff (or where applicable the Pastoral Office).
- Staff are not permitted to take photos or videos of pupils on their personal phones. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment should be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

11. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Appendix 1 The Acceptable Use Agreement - Staff and Governors

Preamble

IT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT.

All new staff are expected to sign this policy on appointment and adhere at all times to its contents, including any variations as may be made from time to time. Current staff will have the opportunity to acknowledge this updated version through their IT account. This work forms part of our terms and conditions.

Any concerns or clarification should be discussed with the Headteacher or the **online safety coordinator.**

Scope

This AUP applies to the responsible use of the school's IT resources and any related technologies.

1. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
2. I will ensure that all electronic communications with students and staff are compatible with my professional role.
3. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
4. I will only use the approved, secure e-mail system(s) for any school business.
5. I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted if on a pen drive/device.
6. I will not purchase or install any hardware of software without first consulting the IT Technicians or the SDITL.
7. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
8. Images of students and/ or staff will only be taken, stored on the school IT system and used for professional purposes in line with school policy and with the consent of the parent, carer or staff member.
9. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, or Headteacher.
10. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
11. I will respect copyright and intellectual property rights.
12. I will ensure that my use of school IT resources, both in school and outside school, will not bring my professional role into disrepute. Please refer to the Code of Conduct.

13. I will support and promote the school's online safety and Data Protection and security policies and help students to be safe and responsible in their use of IT and related technologies.
14. I understand this forms part of the terms and conditions set out in my contract of employment.
15. I will not allow any other user to access my school IT account. The exception would be if the IT Technician or similar support service needs to resolve problems.
16. I understand that all school-owned equipment and devices must only be used by school employees.
17. I will use my school Google school account only for school Google work / apps.
18. If I connect a mobile device (e.g. laptop or USB device) to the school network or a school device, I agree to the school systems accessing that device and that they may take necessary action, including deleting.

New User Signature only

I agree to follow this code of conduct and to support the safe and secure use of IT throughout the school.

Signature …… Date ……

Full Name ……..(printed)

Job title . . . . . .

Appendix 2 The Acceptable Use Agreement – Pupils

Each school's AUP is based on the points below and described using age-appropriate language.

Preamble

- IT - in all its forms - is part of our daily life in school.
- This agreement makes students aware of their responsibilities when using IT in all its forms.
- All students have a school IT account which is for their *sole* use only and for which they are responsible.
- All pupils must abide by these guidelines, including any variations as may be made from time to time.
- All new students will sign this document as part of the enrolment form and process.
- All current students will acknowledge it as part of using their IT accounts annually.

Any concerns or queries should be discussed with the Headteacher or the online safety coordinator.

Scope

This agreement applies to all students at the school and their use of personal and school owned devices.
This is designed to keep students safe. The school Behaviour Policy sanctions will apply as necessary for any deliberate misuse of IT.

1. I will make sure that all my IT communications are responsible and sensible. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
2. I will only use IT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
3. I will only log on to the school network or other resources with my own user name and password. I will not let anyone else use my account.
4. I will not reveal my passwords to anyone.
5. In school I may only use my school email address as the only email account used for any communications on school issues.
6. I will report problems that I have to the school via my teacher or an IT Technician.
7. I will treat school IT equipment with respect, I understand my parents may be asked to pay for equipment that I damage.
8. I will not download or install software on school technologies. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I come across any such material I will report it immediately to my teacher.
9. I will not give out any personal information such as name, phone number or address.
10. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
11. Images of students and / or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the class teacher.

12. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress, nor bring the school into disrepute.
13. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
14. I will respect the privacy and ownership of others' work on-line at all times.
15. I will not attempt to bypass any security on school systems, or make use of material that is not intended for student use.
16. I understand that all my use of the computers, the internet and other related technologies can be monitored and made available to my teachers or parents.
17. I will use my Google school account (if I am issued with one) only for school Google apps.
18. If I connect a mobile device (e.g. laptop or USB device) to the school network or a school device, I agree to the school systems accessing that device and that they may take necessary action.

New User Signature only
Signed:

Print Name:

Date:

Appendix 3 Acceptable Use Agreement - Parents

Dear Parent/ Carer,

Information Technology including the internet, learning platforms, e-mail and mobile technologies has become an important part of learning in our school. We expect all students to be safe and responsible when using any IT. It is essential that students are aware of safety and know how to stay safe when using any IT.

Students are expected to read and discuss this agreement with their parent or carer and then to follow the terms of the agreement, including any variations as may be made from time to time.

Any concerns or explanation can be discussed with their form or class teacher or with the online safety coordinator or the Headteacher.

Please read Appendix 2 with your child and sign this section of the form before returning it to the school. Please be aware that acceptance of a place at any school within the St John the Baptist CMAT and enrolment of your child constitutes your acceptance and support of the IT Acceptable Use Agreement, as valid with changes from time to time, and all other school policy and procedures.

✂----------

New Parent/ carer signature

I have read this document and will support my son/daughter in following the Acceptable Use agreement to support his / her safe and responsible use of IT while at a school within the St John the Baptist CMAT.

Parent/ Carer Signature …….

Student Name…….

Class / Form …….. Date ……

Appendix 4 Photo permission form for new parents

St John the Baptist CMAT believes that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of pupils for internal display and displaying pupil work enables us to celebrate individual and group successes as a school community.

We would also like to use photographs and videos of the school and its pupils to promote the good educational practice of the school.

Children's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

By signing this form you are consenting to the use of images of your child being used in the following outlets under the terms outlined in our online safety policy:

- All school publications
- On the school website
- In newspapers as allowed by the school
- In videos made by the school or in class for school projects

This consent form covers consent for the duration of your child's time at the school.

Once your child leaves the school, photographs and videos may be archived within the school but will not be published without renewed consent. More information regarding the storage and protection of images can be found in the school **Data Protection policy**.

A full copy of the school's policy on online safety containing information on the safe use of photographs, videos, and the work of children in school can be found in the school office and on the MAT website.

Parental permission signature required

Can we use your child's photograph?

- in printed publications by school within St John the Baptist CMAT
- on our website, school blogs, or the school's partnership websites either:
    - In a group or as a member of a whole school activity
    - Individually
- for publication in a newspaper
- and video your child within school, and display these publicly within the school, as part of the curriculum and in class
- and videos of your child to share good practice with professionals from other

If yes, please sign here and return:

Signed: ..... Date: .....

PRINT NAME:……

Appendix 5 The IT Services Code of Conduct

Preamble
The school employ specific staff to administer, develop and run the school IT systems. Of necessity these staff have sweeping powers and access rights across the systems which are needed for effective day to day running of the network. This document lays out a code of conduct for those staff. This document is in addition to the standard Code of Conduct.

Scope
This Code of Conduct applies both to the staff that specifically support the wider school IT network and resources and also to those who have authority over specifics applications, systems or web resources with regard to those specific resources.

Authority
The Headteacher and the Local Governing Body delegate full authority for accessing, managing and running the school IT network and associated system to the IT Services Manager / IT Technician. He in turn delegates that authority to members of the IT team as needed to perform their duties. This authority will not be delegated outside the IT team without the Headteacher's permission.

Confidentiality
During the course of their work, administrators are likely to become aware of information which is or may be regarded as confidential. Unless it raises a safeguarding concern, any such information must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation or legitimate authorised request.
Administrators may not browse areas of the network or school resources for any purpose than fulfilling their job.

Assumed Authority
If a user requests assistance from the IT team, the user's authorisation to access those areas covered by the issue being investigated will be assumed. This authority will extend no further than that required to deal with the specific issue.

Access to personal areas
In exceptional circumstances a member of staff's line manager or the headteacher may request temporary access to areas normally accessible only to that user (e.g. email or home folders). All such request s must be logged so they can be reported on at a later date if required.

System Logins
System logins will only be created for staff and pupils who have passed through the approved admission and authorisation channels. In practice this means they will need to have an entry on the school MIS system. Guest users may be granted temporary access for limited, defined periods of time with no access allowed to staff resources. Other access arrangements must be approved on a case by case basis by the Headteacher and recorded.

Access to school IT resources and files
Authority for access to files and resources that the school owns is delegated to the managers of the respective departments or persons who are otherwise responsible for those resources. Permission must be sought and obtained from them or the headteacher before access is granted.

Exceptional Circumstances
In exceptional circumstances where immediate action is required to protect the network, data or any person or if no one is available to give authorisation (e.g. during school holidays), the IT team may act without such authority. All such instances of such action must be reported to the Headteacher at the earliest opportunity.

Appendix 6 Network Etiquette and Privacy – A Guide

All members of our school communities are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

BE POLITE. Never send or encourage others to send abusive messages.

USE APPROPRIATE LANGUAGE. Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

PRIVACY. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.

PASSWORD. Do not reveal your password to anyone. If you think someone has obtained your password, change it, and contact a member of the IT Team or your teacher.

ELECTRONIC MAIL. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.

DISRUPTIONS. Do not use the network in any way that would disrupt use of the services by others.

OTHER CONSIDERATIONS:

- Be brief. Few people will bother to read a long message. Proof read your message to ensure that it is error free and easy to understand.
- Remember that humour and satire are very often misinterpreted.
- Cite references for any facts that you present. Do not copy work and imply that it is your own. If you do so you are almost certainly guilty of plagiarism. Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.
- Respect the rights and beliefs of others.

Appendix 7 Model Union Guidance

ONLINE SAFETY: PROTECTING SCHOOL STAFF

This document provides a brief guide on how to stay 'Cybersafe'.

Online safety is a key issue for all schools as it can pervade all aspects of school life. Staff in schools, as well as pupils, may become targets of 'cyberbullying'. Cyberbullying is a whole school community issue. It takes place when an individual or group of people use technology such as the internet, mobile phones, e-mail, chat rooms, or social networking sites to bully, threaten or embarrass their victim. It is important that schools make it clear that bullying including cyberbullying of staff is unacceptable.

The following information provides the 'do's and don'ts' on how to stay 'Cybersafe', taking into account the unique position that a teacher or support staff member has in the school and wider community:

Teachers / Support Staff should

- not post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see;
- not leave a computer logged in when you are away from your desk and keep passwords secret and protect access to accounts;
- not befriend pupils or ex pupils of school / college age on social networking sites,. (You should also consider carefully the potentially adverse implications of befriending parents or adult ex-pupils – indeed DfE advice is to not befriend ex pupils at all. There are clear reputational and other risks associated with linking with parents and / or adult ex pupils on social networking sites and the member of staff is advised to make themselves as fully informed as possible of those risks, for example by speaking with the Headteacher)
- keep personal phone numbers private and not use your own mobile phones to contact pupils or parents;
- use a school mobile phone when on a school trip;
- keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible;
- ensure that school rules regarding the use of technologies are consistently enforced;
- not personally retaliate to any incident;

- report any incident to the appropriate member of staff in a timely manner (usually a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of cyberbullying incidents);

- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material, including the URL or web address;

- use school e-mail address only for work purposes;

- be aware that if you access any personal web-based e-mail accounts via your school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance;

Teachers / Support staff should recognise that laptops provided by the employer are for employer's business only, and are not the personal property of staff and therefore should not also be used by family members or for personal activities. Schools should make reasonable attempts to ensure that staff know the risks and dangers of inappropriate internet use

Useful Resources

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material the staff member should use the tools on the social networking site directly to make a report. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is, for example by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected to be illegal you should contact the police directly.

Contact details for social networking sites
The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. Advice can be found here
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/safety-tools-on-online-services

Facebook Read Facebook's rules Report to Facebook Facebook Safety Centre	**YouTube** Read YouTube's rules Report to YouTube YouTube Safety Centre
Instagram Read Instagram's rules Report to Instagram Instagram Safety Centre	**Twitter** Read Twitter's rules Reporting to Twitter
Vine Read Vine's rules Contacting Vine and reporting	**Kik Messenger** Read Kik's rules Reporting to Kik Kik Help Centre
Ask.fm Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.	**Tumblr** Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. They can help you to change the number of the person being bullied if necessary. It is not always possible for operators to block particular numbers from contacting the person being bullied, but many phones, such as IPhones allow users to block phone numbers.

If you want to prosecute the individual contact the police. If a bully is making direct threats which you feel constitute a real danger, phone 999. If there isn't an immediate danger, then contact the non-emergency number 101. The mobile provider can work closely with the police and can usually trace malicious calls for them.

Contact details for service providers:

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Appendix 8 Relevant policies

- Anti-Bullying policy
- Behaviour For Learning policy
- Disclosure and Barring Service (DBS) procedures
- Prevent policy
- Safer Recruitment policy
- Staff Code of Conduct
- Staff Use of the internet
- Whistle-Blowing policy

Appendix 9 – Specific role description within Notre Dame High School

2.3 E-Safety Coordinator

- The E-Safety coordinator is the Head of Computing.
- Liaises with and reports to the IT Steering Group.
- Liaises with the PSHE Coordinator to ensure effective e-safety curriculum provision across Years 7-13 e.g. through the IT Curriculum, the PSHE curriculum; Induction Days; or use of Form-time. This can also include the use of pop-ups as reminders.
- Works in partnership with the SDITL, DFE, CEOP, and the Internet Service Provider and school IT Manager to ensure systems to protect students are reviewed and improved.
- Ensures the school IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly – in liaison with the IT Services Manager.
- Receives updates of e-safety incidents and creates a record of type of incidents to inform future e-safety developments and use this to inform e-safety training to the school community.
- Liaises with the SDILT, the nominated member of the Governing Body & the Headteacher to provide an annual report on e-safety.

Appendix 10 Critical Security Control (taken from the NCC Model Online Safety policy February 2916)

Critical Security Control	Questions for School Head Teachers, Senior Leaders and Governors
1. Inventory of Authorized and Unauthorized Devices: Actively manage (inventory, track, and correct) **all hardware devices** on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	Does your school's ICT Code of Conduct/acceptable use policy (AUP) include provisions/instructions to ensure only authorised devices are connected to the school's network?
2. Inventory of Authorized and Unauthorized Software: Actively manage (inventory, track, and correct) **all software on the network** so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	Does your school's ICT Code of Conduct/acceptable use policy (AUP) include provisions/instructions to ensure only authorised devices are connected to the school's network?
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Does your school's ICT Code of Conduct/acceptable use policy (AUP) include clear provisions/instructions warning users about tampering with secure configurations, with clear sanctions for any infraction? Do you have visibility of likely costs to upgrade and refresh hardware and software as necessary, and when these costs are likely to be incurred (for example, antivirus software subscriptions, firewall support and maintenance services, dates for when hardware/software will go "end of life" and need to be replaced)?
4. Continuous Vulnerability Assessment and Remediation: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	Do you have processes in place for regular review of e-security functions and your IT acceptable use policies to address new and emerging threats? How do you ensure staff and pupils receive appropriate e-security advice and training?
5. Malware Defences: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the	How do you ensure that your ICT Code of Conduct/acceptable use policy (AUP) are up to date to minimise risks in this area?

use of automation to enable rapid updating of defence, data gathering, and corrective action.	What sanctions are applied for malicious use of school IT services and systems?
6. Application Software Security: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses	Do you have visibility of when significant upgrade and renewal of software will be required, both in terms of likely cost and ensuring service continuity? How do you ensure staff and pupils are trained in the use of new software?

7. Wireless Access Control: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	What is the school's policy on wireless access – do you allow guest access, or access from staff- or pupil-owned devices? Does your ICT Code of Conduct/acceptable use policy (AUP) appropriately encompass access from staff- or pupil-owned devices if this is allowed? Do your staff and pupils understand their obligations and responsibilities in relation to using their own devices in school, if they are allowed to do so?
8. Data Recovery Capability: The processes and tools used to back up critical information properly with a proven methodology for timely recovery.	Does your school have an overarching disaster recovery/business continuity plan? If so, does this encompass restoration of IT facilities and critical school data appropriately?
9. Security Skills Assessment and Appropriate Training to Fill Gaps: For all functional roles in the organization (prioritizing those mission--critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	Does your school's overarching staff training and development planning include provisions to ensure that technical support staff can keep up to date with e-security risks and best practices and that all teaching and administrative personnel understand their own e-security obligations and responsibilities?
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management	Do you have visibility/awareness of when major changes and/or upgrades will need to be carried out, in terms of both likely cost/budgeting and maintaining service continuity?

and change control process in order to prevent attackers from exploiting vulnerable services and settings.	
11. Limitation and Control of Network Ports, Protocols, and Services: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	Do you have visibility of when major changes are likely to be necessary? Do you have effective processes for communicating changes, for example in relation to changing security settings to allow access to a new service or facility – are appropriate risk assessment and management processes in place and adhered to?
12. Controlled Use of Administrative Privileges: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	Do you have effective strategies in place to ensure the importance of administrator privileges are understood and respected? Does your ICT Code of Conduct/acceptable use policy (AUP) require strong, complex passwords and regular password changes?
13. Boundary Defence: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	Do you employ any independent third party testing of your boundary defences to maintain their effectiveness in the light of dynamic and emerging threats?
14. Maintenance, Monitoring, and Analysis of Audit Logs: Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.	How do you ensure that sufficient time is allocated to reviewing and acting upon the outputs from monitoring and logging activities? Where do responsibilities for reviewing outputs from monitoring and logging reside? What are your data retention policies, and where are they described?
15. Controlled Access Based on the Need to Know: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	Does your ICT Code of Conduct/acceptable use policy (AUP) differentiate between the obligations and responsibilities of different groups of users (teaching staff, administrative/managerial staff, pupils, governors)? How do you communicate with and keep different user groups up to date with their obligations and responsibilities?
16. Account Monitoring and Control: Actively manage the life-cycle of system and application accounts – their creation, use,	Do you undertake any monitoring of user accounts for unusual usage?

dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	How do you communicate with, educate and inform different user groups of their obligations and responsibilities?
17. Data Protection: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information (exfiltration: the unauthorized release of data from within a computer system or network)	Are all staff and pupils aware of all their responsibilities and obligations in relation to sensitive and personal data, particularly in the light of schools' roles as data controllers under The Data Protection Act 1998?
18. Incident Response and Management: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	How regularly are incident handling processes reviewed? Do you undertake any example incident scenarios to test and update incident handling processes and procedures?
19. Secure Network Engineering: Make security an inherent attribute of the enterprise by specifying, designing, and building--in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	How much and how often are time and resources allocated to reviewing and updating the school network as a whole? What processes and analysis are employed to determine which security functions are best provided in house and which should be delivered using the expertise of third parties such as broadband service providers?
20. Penetration Tests and Red Team Exercises: Test the overall strength of an organization's defences (the technology, the processes, and the people) by simulating the objectives and actions of an attacker	How do you identify sources of advice and support that can scrutinise the security of you network and suggest an action plan for improvement?

Appendix 11 Guidance for schools: Parents & Carers use of photography and filming at school events

Parent/carers use of photography and filming at school events and the way that they subsequently chose to use these images is sometimes a difficult area for schools to manage. Our practice has to take into consideration the Information Commissioner's Office (ICO) guidance whilst aiming to protect vulnerable pupils. With this in mind, some schools have identified a need for guidance in preparation for the end of term Christmas activities.

Parents and carers may wish to photograph or make video recordings of their children taking part in school events as these images are an enduring part of each family's record of their child's progress and a celebration of success and achievement. The Data Protection Act 1998 does not apply to images taken purely for personal use and therefore parents and carers are exempt from the provisions of the Act if they are taking photographs or making a video recording for **their own private use**. The Information Commissioner's Office guidance makes it clear that the Act should not be used as a reason to stop parents or family members from photographing or recording school events.

When the Act applies and when it does not:

Personal use:

1. A parent takes a photograph of their child and some friends taking part in the school sports day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.

2. Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official school use

1. Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

2. A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use

A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act

Whilst the ICO guidance clarifies the issues surrounding parental photography and data protection, it does not provide clarity on how schools can manage some of the safeguarding issues that are related to photography of school events. An example may include:

A parent/carer has posted a photograph of the school production on a social networking site. Whilst the photograph has been taken to celebrate the achievement of their child, it includes other pupils at the school including a child who has moved to the area because their parent has fled a violent parent. The photograph will identify the child, the family's whereabouts and may place both child and parent in considerable danger.

We must always be mindful of the need to safeguard the welfare of children in our schools, and issues of child protection, data protection and parental consent will need to be given careful thought. Whilst aiming to include all pupils in these productions and events, every effort should be made by the school to prevent capturing of the image of any child who should not be identified or whose parent has not given consent for their images to be captured.

Here are some practical steps you could take to ensure that images of children are taken and used safely:

- Make sure you remind parents about your school's policy and let them know that you are ready to listen and take seriously the concerns of individual parents.
- Include a section in the consent form to indicate that any images parents take during school activities will not be used inappropriately.
- Include a statement on parental responsibility for appropriate use of images in the relevant school policy.
- Ask parents or legal guardians for permission for their child to be included in images taken by other parents whose children are also participating in the same school event. Ask every year in the standard school communication if parents wish to change their permission.
- Include a section in the consent form to indicate that any images parents take during school activities will not be used inappropriately.
- If they are allowed, they should be advised only to take photos of their own child or to seek permission of other parents if they wish to take photographs of the whole cast.
- Photos, if taken, should only be used for the family's own album and should not be posted on websites.
- Many schools have found it useful to ask parents not to film or take photographs during the performance but to set aside time at the end for parents to photograph their child.
- Parents can get upset by the suggestion that one of them may use the images inappropriately; it might be useful to advise them on the safe use of social networking sites and the implications of posting photographs and videos.
- Many parents have mobile phones with very good cameras. You can ask parents to switch off their phones during the performance. This would be simple good manners anyway, but it would be virtually impossible to police the event for mobile phone cameras.

- 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.

Further information & Advice

- ICO - **Taking Photographs in Schools**
- ICO – **Social networking.**
- E-Safety Toolkit