TRINITY CATHOLIC COLLEGE & SIXTH FORM
An inclusive, learning community living out Gospel values

NICHOLAS POSTGATE Catholic Academy Trust

TRINITY CATHOLIC COLLEGE & SIXTH FORM

E-Safety Policy

Adopted by Trinity Catholic College
Reviewed & Approved by Governors : March 2018
Next Review: March 2019

"An Inclusive Learning Community Living out Gospel Values"

Contents

Scope

This policy applies to all members of the Trinity Catholic College community (staff, students, volunteers, parents, governors, wider community) who have access to and use the College ICT facilities either onsite or as a remote user.

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

Roles and Responsibilities

Every adult member of the school community who has a responsibility towards the welfare of the students has a responsibility towards keeping the students safe in their use of ICT. This section outlines the different responsibilities of the different groups and individuals

Governing Body

The Governing body are responsible for the approval of the E-Safety policy and reviewing and monitoring the effectiveness of the policy.

Head Teacher & Leadership Team

- The Headteacher responsibility for ensuring the safety (including e-safety) of all members of the College community. The day to day responsibility will be delegated to the E-safety Officer.
- The Headteacher and other designated members of the Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Headteacher/Leadership Team are responsible for ensuring that the E-Safety Officer and other relevant members of staff receive suitable training to carry out their duties
- The Headteacher/Leadership Team will ensure that there is a system for monitoring and supporting those in school who carry out internal e-safety monitoring. This is to provide a safety net and to support those who take on monitoring roles

E-Safety Officer

- Day to day responsibility for e-safety issues and has a leading role in reviewing the e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident occurring
- Provides training, advice and guidance for staff
- Liaises with the Local Authority and other relevant bodies
- Liaises with the ICT technical staff
- Receives reports of and logs e-safety incidents to inform future policy developments
- Meets with E-Safety Governor to discuss current issues, review incident logs and filtering
- Reports regularly to Leadership Team

Network Manager / Technical Support Staff

The Network Manager and technical support team are responsible for ensuring:

- That the network infrastructure is secure and is not open to malicious attacks
- The School meets the required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy in which passwords are secure
- the filtering policies are applied and regularly updated
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety responsibility
- that the use of the network, Internet, CC4 Anywhere remote access and Trinity Cloud is regularly monitored in order that any misuse or attempted misuse can be reported to the E-safety officer
- that monitoring software and systems are implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Trinity Catholic College e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-safety Officer
- All digital communication with students / parents / carers should be on a professional level and ONLY carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies such as computers, mobile phones, cameras etc in lesson and other school activities where allowed.

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

Child Protection Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- inappropriate online communication with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

- Students are responsible or using the digital technology in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations
- Need to know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking of and use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practices when using digital technologies out of school and realise that their actions out of school, if related to their membership of the school, are still covered by the e-safety policy.

Parents / Carers

Parents / carers play a vital role in ensuring that their children understand the need to use digital technology and the Internet in a safe and responsible way. Trinity Catholic College will take every opportunity to help parents understand these issues through parents' evenings, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be encouraged to support Trinity Catholic College in promoting good e-safety practices and to follow guidelines on the appropriate use of

- Digital video and images taken at school events
- access to parents' sections of the website and online student data
- Their children's personal devices (such as mobile phones) in the school where this is allowed

Policy Statements

Education - Students

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (statements will need to be adapted, depending on school / academy structure and the age of the students / pupils)

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

Education - Parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents' evenings
- High profile events / campaigns eg Safer Internet Day

Education and Training - Staff and Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training - Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical - Infrastructure, Equipment, Filtering, Monitoring

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

A more detailed Technical Security Template Policy can be found in the appendix.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the technical team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic year.
- The "administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (eg school safe)
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school / academy will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

BYOD / 6th Form Mobile Device Scheme

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. Currently at Trinity BYOD extends only to staff and students of the 6th form College. See the appendix for the Mobile Device Scheme Acceptable Use Policy. For a BYOD scheme to work, the following principles are in place:

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of Digital Video and Images

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

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

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

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communication Technologies

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

	Staff & Other Adults			Students			
Communication Technologies	Allowed	Allowed at certain times	Selected staff only	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile Phones may be brought to school	🟩				🟩		
Use of mobile phones in lessons							🟩
Use of mobile phones in social time	🟩					🟩	
Taking photos on mobile phones/cameras		🟩					🟩
Use of other mobile devices eg tablets	🟩						🟩
Use of personal email addresses in school or on school network		🟩		🟩			
Use of school email for personal emails		🟩				🟩	
Use of messaging apps		🟩		🟩			
Use of social media		🟩		🟩			
Use of blogs		🟩					🟩

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive,

discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party.
Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Staff use of social media for educational purposes must comply with the social media policy

Unsuitable / inappropriate Activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and Illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate, pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					🟩
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					🟩
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					🟩
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					🟩
	pornography				🟩	
	promotion of any kind of discrimination				🟩	
	threatening behaviour, including promotion of physical violence or mental harm				🟩	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				🟩	
Using school systems to run a private business					🟩	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					🟩	
Infringing copyright					🟩	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					🟩	
Creating or propagating computer viruses or other harmful files					🟩	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					🟩	

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

Responding to Incidents

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

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

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendices

- Student AUP - 11-16
- Student on-screen AUP
- Student e-Safety Rules
- Parents/Carers AUP
- Student AUP - 6th form Mobile Devices Scheme
- Staff/Volunteers AUP
- Staff social media use guidance
- Legislation

Student Acceptable Use Agreement for the use of ICT

School / Academy Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal use unless I have permission.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or change any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images or videos of anyone without their permission.

I understand that the school has to make sure that the ICT systems are secure and run without problems:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to inappropriate materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I use is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school / academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, inclusion, suspension, contact with parents and in the event of illegal activities involvement of the police.

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

Student / Pupil Acceptable Use Agreement Form

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

I have read and understand the above and agree to follow these guidelines when:

- I use the school / academy systems and devices (both in and out of school)
- I use my own devices in the school / academy (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school / academy eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student::	
Tutor Group:	
Signed:	
Date:	

Staff on-screen AUP

- All ICT activity should be appropriate to staff professional activity or the student’s education and in line with the Trinity Catholic College E-Safety Policy
- Internet access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As E-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- The usefulness and integrity of the system or its contents should not be intentionally compromised by the user.
- Use of the network to access inappropriate material such as pornographic, racist or offensive material is forbidden.

Student e-Safety Rules (Same as Y6 induction handbook)

The school has computers with Internet access to help you learn. These rules will help keep you safe and protect others.

- I will only access the system with my own username and password; which I will keep secret.
- I will not access other people’s files.
- I will use the computers for valid reasons.
- I will arrange to be supervised by a member of staff before using the Internet.
- I will only E-mail people I know, or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number or arrange to meet someone unless my parent, carer or teacher has given me permission.
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Parent / Carer Acceptable Use Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that students / pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools / academies will need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

Permission Form

Parent / Carers Name____________________________Student / Pupil

Name_________________________

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

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

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

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

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

Signed ____ Date_____________________

Mobile Device Scheme AUP

Mobile Device Scheme Acceptable Use Policy (AUP)

Introduction

This document details the rules and responsibilities which govern the correct use and care of the device (iPad or Laptop). Before you take delivery of your device it is essential that you read, understand and sign this document. It is your responsibility to follow these guidelines for the correct use of the device and understand that failing to do so may result in Trinity Catholic College requesting that you return the device.

Use of the device

The purpose of this scheme is to provide you with the opportunity to have a mobile device that you can use to enhance your education. As such you are permitted to use the device both at home and in college for educational and personal use. There are however strict guidelines that must be followed during the payment period.

1. Do not install illegal software (anything that has not been purchased legitimately including computer games)
2. Do not install download software (such as Torrent applications)
3. Do not store illegal music or films (if you have not purchased it, then it is illegal)
4. Do not install different operating systems on the laptop such as Linux
5. Do not Jailbreak the iPad
6. Do not share log in details with other people
7. Do not remove the asset tag from the device

If your device requires a repair in which it is sent back to the manufacturer, failure to follow the above rules may mean that your warranty will have been cancelled. In the case of illegal software, music or films you can run the risk of prosecution if the manufacturer passes the device to the authorities.

Looking after the device

You are responsible for the safekeeping of the device and ensuring that it is kept in good working order. If you are intending on transporting the device regularly it is worth investing in a protective case or bag. If the device needs to be returned to the college it is vital that it is in ‘as new’ condition.
The following guidelines must be followed to ensure that the device is correctly looked after.

1. Do not stick stickers to the device
2. Do not paint or draw on the device
3. Do not intentionally scratch or mark the device
4. Do not attempt to take apart, modify or repair the device
5. Keep the device safe in a protective case or bag
6. Do not lend the device to another person without supervising their use
7. Always report any damage immediately to the college

Use of the Internet

In College

In college you are able to access the Internet using our Wi-Fi network. You need to be responsible when accessing the Internet in college and understand that your use of the Internet is monitored and can be blocked if necessary. The following guidance must be adhered to when using the Internet in college

1. Do not attempt to use proxy bypass sites or other means to bypass the College’s Internet security
2. Do not use the Internet for purposes that may cause upset to others or put others at risk
3. Use common sense when browsing the internet and the content that you search for (remember that even though a search may be blocked, the network will still record what you searched for)

At home

At home you will be able to access the Internet using your own home broadband. Please not that this is **NOT** provided through this scheme. Although you are using your own Internet connection please note that the device will still report inappropriate use of the internet back to college.

End of Payment Period

At the end of the payment period the college will ‘hand over’ the device to you. From this point ownership will pass from the college to you. If this is at the end of the 2 year period the following will happen

1. The insurance policy will come to an end
2. The warranty period will come to an end
3. Any repairs will become your responsibility

For the transfer of ownership to take place you must complete and sign the End of Term document

CC4 Anywhere Acceptable Use Policy (Student Policy)

Description

‘CC4 Anywhere’ is a system that allows remote access from any location with an Internet connection, at any time, to the school network, files and programs.
The system provides remote access to:

- Microsoft Office
- Personal Files (your user area)
- Shared Files
- Other software applications held within the school

Essential Guidance on Usage for CC4 Anywhere

As the system allows you access to the school network from outside of the school building it is essential that good e-safety and data protection practice is adhered to.

1. Your user name and password must be kept secure and not shared
2. Your password should not be easily guessed and contain a mixture of text, numbers and special characters to make it more secure
3. CC4 anywhere should only be used on your school laptop, iPad, school computers or home computer (not public systems such as a library) and never left unattended
4. You must always log off once you have finished your session or lock the session if you are leaving your computer for brief periods

Declaration

In taking part in the Sixth form mobile device scheme, I have read and understand this Acceptable Use Policy (AUP)

Please sign to show that you have read and understand this guidance

Name ____

Signed ____

Date ____

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school / academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, Google Apps etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school / academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / Shared on Google Apps) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school / academy equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date antivirus software and are free from viruses.
- I will not use personal email addresses on the school / academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy.. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

I will ensure that I have permission to use the original work of others in my own work
Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school / academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Staff Social Media Guidance and Use (Twitter)

Social Networking

As with most social networking sites, there are incredible educational benefits that can be gained through proper and correct use. There are however so many risks that MUST be considered before engaging with students through these sites. As a teacher, these risks can potentially:

- Damage your reputation
- Put you in compromising positions
- Be career ending
- Result in criminal charges

Each Social networking site presents its own unique problems through the nature of how the sites work but regardless of the site, the most important thing is that you and the students are safe and not placed in a position that compromises anyone.

As a result of the potential risks, there are only 2 social networks that are permitted. These are

- Twitter
- Google+

Guidelines for use of Twitter

If you are choosing to use Twitter with students then the following guidance must be adhered to

- Never use your personal twitter account - create a new one for school use
- Never follow the students – if you follow the students then you will see their personal posts
- If students want to send you a message they just need to include your @name in the post
- If you want to send a message to a specific student, include the @name in your post, this way the message is still seen by all of your other followers
- Never post anything that compromises you and is of a personal nature
- Set the account to private so that only your followers can see your posts and you confirm anyone who chooses to follow you
- REMEMBER – Twitter is a public site with very few restrictions. If you have a personal twitter account, students can easily find you and follow you – consider what you post, who will see it and changing your settings to private

Examples of Twitter used with students at Trinity

@jthynneTCC – Mainly used with Y12 and 13 Applied ICT

@trinityccbus – used with Y12 and 13 Applied Business

Are you considering using Twitter?

If you are considering using Twitter with students could you please arrange to meet James Thynne for 15 minutes to ensure that all settings are correct and that there is a formal record of your use of Twitter– ultimately we need to take every step possible to ensure that there are no potential risks to staff and students.

Naming Conventions

In the interest of keeping some form of structure (as far as is possible with Twitter), the following naming convention needs to be applied as the maximum username Twitter will allow is 15 characters

Group/Department/Project Twitter Account

- @TCCname

Individual Staff Account

- @nameTCC

Guidelines for use of Google+

Google+ is a lesser used social network that is linked to our school Google Apps for Education accounts. Google+ is easy to control and uses ‘communities’ and ‘circles’ of friends to control privacy. As with all social networking sites, it is important to be careful, consider what you post and who can see it.

Google+ is not widely used by a broad audience (like facebook) as it has not managed to break the market in the same way. It is however excellent for building your own PLN (Personal Learning Network) to connect with other educators and there are many vibrant communities with a wide range of interests from technology to history.

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the event of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 1998

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

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

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

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

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations