E-SAFETY POLICY

AIMS

- To create an environment where students, staff, parents, Academy Representatives and the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.
- To enable to students learn creatively and effectively and encourage collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Students, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.

These agreements and their implementation will promote positive behaviour, which can transfer directly into each student's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer internet usage, year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Signature: **Chair of Academy Representatives**	Name:	Date:
Signature: **Head of School**	Name:	Date:

Our Vision

Saint Augustine's Catholic High School) embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. Saint Augustine's Catholic High School, part of Our Lady of Lourdes Catholic Academy aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

E-Safety Policy Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned and used by adults and young people while on the school premises.

Related Documents:

- Acceptable Use Policy for Staff
- Acceptable Use Policy for Students
- Social Media Policy
- Data Protection Policy
- Behaviour Policy
- Worcester County Council filtering Policy

Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable internet use policy or other in the light of e-safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or students in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police.

Publicising E-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.st-augustines.worcs.sch.uk and the Portal.
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year and whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information at parents evenings and through the school newsletter

Reviewing and evaluating e-safety and ensuring good practice

The Principal / Head of School and Academy Representatives have ultimate responsibility for establishing safe practice and managing E-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to a member of the Senior Leadership Team as our Designated Safeguarding Lead. He is the central point of contact for all e-Safety issues and will be responsible for day to day management. The school has a safeguarding committee which includes all aspects of safeguarding (including e-safety) which discusses policy review and newly introduced legislation bi-annually. The current members are: the Head of School, the Assistant Principal for Pastoral Care, the Deputy Safeguarding Lead, the New Technology Manager (where necessary) and the Safeguarding Academy Representative. (Refer to the E-safety appendix for current role holders.)

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the E-Safety coordinator (Damon Gariff) using the school procedures: (My Concern)
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Physical Environment/Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system, consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Worcester County Council. All staff and students understand that if an inappropriate site is discovered it must be reported to the New Technology Manager who will block the site through Smoothwall. All incidents will be recorded through an incident report on SIMS for audit purposes.
- Requests for changes to the filtering will be directed to the New Technology Manager in the first instance who will add these to Smoothwall and liaise with the e-Safety co-ordinator as appropriate. Change requests will be recorded by the New Technology Manager for audit purposes
- Additionally the school uses Smoothwall to provide further filtering and enable the school to block websites immediately and records the history of websites visited for each pupil.
- The school uses Policy Central on all school owned equipment to ensure compliance with the Acceptable Use Policies.
    - Students use is monitored by the New Technology Manager
    - Staff use is monitored by the New Technology Manager and passed to the Principal / Head of School

- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary usernames and passwords and the details recorded in the ICT Services Helpdesk.
- All students are issued with their own username and password and understand that this must not be shared.

Mobile/emerging technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- Students understand that their mobile phones must be turned off during directed time and used in line with school policies at all other times.
- The Educations and Inspections Act 2006 grants the Principal / Head of School the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Principal / Head of School will exercise this right at his discretion
- Pictures/videos of staff and students should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

E-mail

The school e-mail system is provided, filtered and monitored by Worcester County Council filtering and is governed by Worcester City Council E-mail Use Policy.

- All staff are given a school e-mail address and understand that this must be used for all professional communication
- All students are given a school e-mail address that can be used for educational purposes
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Students may be given the opportunity to check their own e-mail outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible.

Published content

The Principal / Head of School takes responsibility for content published on the school web site.
The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses
- The school does not publish any contact details for the students
- The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school web site or creates a school account on the site

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or students before any images or video are published or distributed outside the school.

- Photographs will be published in line with Government guidance (www.education.gov.uk) and not identify any individual student.
- Students' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to students taking part in external video conferencing.
- Students understand that they must have their teachers permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the students

Social Networking and online communication (see Social Media Policy for further advice)

The School has chosen not to allow use of social networking sites and online communication including Facebook, Instagram, Twitter, Bebo or MySpace.
Guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Students are given age appropriate advice and guidance around the use of such sites.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material.

- Where appropriate, links to specific web sites will be provided instead of open searching for information.
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind students of the Acceptable Use Polices before any activity.
- Staff and students will be expected to reference all third party resources that are used

E-Safety training

- E-Safety is embedded throughout the school curriculum and visited by each year group.
- Students are taught how to validate the accuracy of information found on the internet.
- Assemblies are carried out systematically throughout the year.
- The school will provide parent sessions to provide regular advice and guidance as appropriate.
- Staff training is carried out through inset days, twilight sessions and in morning briefings.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998
Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines

Wider Community

Third party users (eg Academy Representatives, supply teachers and school clubs) of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying, Child Protection Policy, Data Protection Policy, and Acceptable Use Policy.

- Any suspected illegal activity will be reported directly to the police. Worcester County Council will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Principal / Head of School.
- Breaches of this policy by staff will be investigated by the Principal / Head of School action will be taken under Worcester City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All

monitoring of staff use will be carried out by at least 2 senior members of staff (Principal / Head of School and one other member of SLT)

- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti bullying and child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. Referral to Heads of Year may be appropriate at this level. Heads of Year will also deal with email alerts generated by Policy Central for students. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor student offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The *Educations and Inspections Act 2006* grants the Principal / Head of School the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

E-Safety Policy Appendix

Current Role Holders, as of January 2018

E-Safety Coordinator:	**Damon Gariff**
Assistant Principal for Pastoral Care:	**Damon Gariff**
Deputy Safeguard:	**Claire Bird**
New Technologies Manager:	**Ben Glover**
Safeguarding Academy Representative:	**Cecilia Hubble**