St. Gregory's Catholic High School

E Safety Policy

Monitoring

The implementation of the policy will be monitored by the Deputy Headteacher (Pastoral)

Evaluation

The policy was reviewed by the Deputy Headteacher and SLT on 26th October 2020 prior to the submission of the policy to Governors' Community Committee for scrutiny and recommendation to the Full Governing Body for approval.

Policy Review Dates:

Date last approved by Full Governors: 10th December 2019

Date submitted to Governors Committee: 29th October 2020

Date submitted to Full Governing Body: 9th December 2020

Review Frequency: Annually

Start date for policy review: July 2021

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Gregory's Catholic High School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Gregory's Catholic High School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope

This policy applies to all members of St Gregory's Catholic High School community (including staff, students, Governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Gregory's Catholic High School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

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

Role	**Key Responsibilities**
Headteacher	• takes overall responsibility for e-safety provision • takes overall responsibility for data and data security (SIRO) • ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements • is responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • is aware of procedures to be followed in the event of a serious e-safety incident. • receives regular monitoring reports from the E-Safety Co-ordinator • ensures that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)
Designated Safeguarding Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with school ICT technical staff • communicates regularly with SLT and the designated Governor and committee to discuss current issues and practices • ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • ensures that an e-safety incident log is kept up to date • facilitates training and advice for all staff • attends safeguarding team meetings to discuss issues, update actions, review procedures • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming

	• cyber-bullying and use of social media • ensures monitoring of web filter

Role	Key Responsibilities
	• Ensure that parents are regularly updated regarding E safety issues
Governors	• ensures that the school follows all current e-safety advice to keep the children and staff safe • approves the E-Safety Policy and reviews the effectiveness of the policy and its practices. This will be carried out by the Chair of Governors / Community Committee receiving regular information about e-safety in conjunction with the role of a safeguarding Governor • supports the school in encouraging parents and the wider community to become engaged in e-safety activities
Curriculum Leader	• oversees the delivery of the e-safety element of the Computing curriculum liaises with relevant staff regarding policy and practices

Network Manager	• reports any e-safety related issues that arises, to the e-safety coordinator.
	• ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) ensures the security of the school ICT system
	• ensures that:
	  • access controls / encryption exist to protect personal and sensitive information held on school-owned devices
	  • the school's policy on web filtering is applied and updated on a regular basis
	  • ensures that relevant staff are informed of web filtering reports
	  • keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
	  • the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Head teacher / DSL for investigation / action / sanction
	• ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
	• keeps up-to-date documentation of the school's e-security and technical procedures
	• ensures that all data held on students within the Learning environment is adequately protected
	• ensures that all data held on students on the school office machines have appropriate access controls in place

Teachers (Use of ICT within curriculum delivery)	• embed e-safety issues in all aspects of the curriculum and other school activities • supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)

Role	Key Responsibilities
	• ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • report any suspected misuse / problems / concerns to the safety coordinator
All staff	• read, understand and help promote the school's e-safety policies and guidance • read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • report any suspected misuse or problem to the DSL • maintain an awareness of current e-safety issues and guidance • model safe, responsible and professional behaviours in their own use of technology • ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms including email, text and mobile phones • read this policy in conjunction with all related safeguarding policies and reinforce the school policy in regards to mobile phones and related devices • follow additional advice and guidance which may be provided to supplement this policy during the academic year which includes: what every teacher needs to know about E-Safety; What every teacher needs to know about Social Media / Digital Literacy / Friendly WiFi
Students	• read, understand, sign and adhere to the Student Acceptable Use Policy • regularly review the conditions of use on screen by agreeing to our Acceptable Use Agreement • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • understand the importance of reporting abuse, misuse or access to inappropriate materials • know what action to take if they or someone they know feels worried or vulnerable when using online technology. • know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • know and understand school policy on the taking / use of images and on cyber-bullying. • understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • help the school in the creation/ review of e-safety policies

Role	Key Responsibilities
Parents/carers	• support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • read, understand and promote the school Pupil Acceptable Use Agreement with their children • access the school website in accordance with the relevant school Acceptable Use Agreement. • consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the school website / staffroom noticeboard
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with students at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in student and personnel files
- All updates and amendments will be communicated accordingly

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Pupil Progress Manager / E-Safety Coordinator / DSL / Headteacher;
  - confiscation (mobile phone /and hand held device)
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - fixed term exclusion
  - referral to LA / Police.

- Any complaint about staff misuse is referred to the Headteacher / DSL.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy

- Complaints related to child protection / safeguarding are dealt with in accordance with related school policies / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies including safeguarding, AntiBullying, CSE and Behaviour.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been reviewed by the DSL and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Student e-safety curriculum

St Gregory's Catholic High School

- Has a clear, progressive e-safety education programme as part of the Computing curriculum and elements which require additional support and training are via Personal Development and related activities / events / speakers. It is built on LA and national guidance including 'Teaching On-Line Safety in School' DFE June, 2019. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- To understand the law in relation to photographs / images / videos / apps / programs

- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- reminds students about their responsibilities through an Acceptable Use Policy which every student will sign and will be displayed at regular intervals when a student logs on to the school network.
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Uses opportunities such as themed days, Parents' Evenings, The Net and website to reinforce safety practices / procedures and to share up to date information.

Staff and governor training

St Gregory's Catholic High School

- Ensures staff know how to send, store, record, receive sensitive and personal data and understand the requirement to protect data where the sensitivity requires data protection;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.
- Appropriate training will be provided for Governors

Parent awareness and training

St Gregory's Catholic High School

- Runs a rolling programme of advice and guidance for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site; distributed at parents evenings
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents
  - Invitations to meetings and events focused on particular elements of E safety

3. Expected Conduct and Incident management

Expected conduct

At St Gregory's Catholic High School, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

At St Gregory's Catholic High School:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed in dealing with e-safety issues ○ monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.

- the Police will be contacted if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

St Gregory's Catholic High School

- Has educational filtered secure broadband connectivity
- Uses filtering which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network health through the use of RMVP anti-virus, and a network set-up so staff and pupils cannot download executable files;
- Uses DfE / LA approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes;
- Has blocked student access to music download or shopping sites – except those approved for educational purposes;
- Uses security time-outs on Internet access where practicable / useful;
- Is vigilant in its supervision of students' use at all times, as far as is reasonable;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures students only publish within an appropriately secure environment;
- Requires staff to preview websites before use and encourages use of the school's Learning Environment as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that all system use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the network manager;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse;

- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities including LA and Police.

Network management (user access, backup)

St Gregory's Catholic High School
- Uses individual, audited log-ins for all users
- Does not issue guest accounts for external or short term visitors;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Ensures the network manager is up-to-date with services and policies / requires the Technical Support Provider to be up-to-date with services and policies;
- Ensures the storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, we:

- Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. We provide staff with an individual network log-in username. They are expected to use a personal password;
- Provide staff access to the school's management information system, controlled via a password for data security purposes;
- Provide students with an individual network log-in username. They are also expected to use a personal password;
- Ensure students have their own unique username and password which gives them access to the learning environment;
- Make clear that no one should log on as another user and make clear that students should never be allowed to log-on or use teacher and staff logins;
- Set-up the network with a shared work area for students and one for staff, using cloud technology. Staff and students are shown how to save work and access work from these areas;
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- Request that teachers and students do not switch the computers off during or at the end of the day. The network should automatically shut down each computer at a designated time, allowing for regular updates to take place;
- Have set-up the network so that users cannot download executable files / programmes;
- Have blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scan all mobile equipment/school assets with anti-virus / spyware before connection to the network;

- Make clear that only school approved equipment, owned by the school, should be connected to the school network;
- Make clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use";
- Make clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintain equipment to ensure Health and Safety is followed; e.g. projector filters cleaned; equipment installed and checked by approved personnel/suppliers;
- Ensure that access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensure that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems;
- Do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems and with the network manager's approval;
- Provide students and staff with access to content and resources through the approved Learning Environment which staff and pupils access using their username and password;
- Make clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Have a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Use the DfE secure s2s website for all CTF files sent to other schools;
- Ensure that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follow ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Ensure our wireless network has been secured to appropriate standards suitable for educational use;
- Ensure all computer equipment is installed professionally and meets health and safety standards;
- Ensure projectors are maintained so that the quality of presentation remains high;
- Review the school ICT systems regularly with regard to health and safety and security.

Password policy

- St Gregory's Catholic High School makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

St Gregory's Catholic High School

- Provides staff with an email account for their professional use. Personal email should be through a separate account;
- Does not publish personal e-mail addresses of students or staff on the school website.
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products RMVP and Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, RM 'Safetynet' filtering monitors and protects our Internet access to the World Wide Web.

Students:

- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments; ○ embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;

- not to arrange to meet anyone they meet through e-mail without having discussed with an adult;
- that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data;
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted; ○ embedding adverts is not allowed;

- All staff sign the school Agreement Form AUP;

School website ○ The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- Uploading of information is restricted to our website authorisers:
- The school web site complies with the statutory DfE guidelines for publications; ○ Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published;
- We do not use embedded geodata in respect of stored images ○ We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning environment ○ Uploading of information on the schools' learning environment is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

- Photographs and videos uploaded to the schools learning environment will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved and closed systems, such as the learning environment;

Social networking ○ Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- 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 personal information being accessed / shared / used
- They do not get involved in any practices / information sharing which will compromise or be seen to abuse their role as educators of young people in their care

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained in house for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

- Named staff only are allowed to view CCTV footage where it is required to support the Health and Safety / Safeguarding and Behaviour of our students
- Access to CCTV data / information is protected under Data Protection and Safeguarding Legislation
- The school follows the Home Office Surveillance Camera Code of Practice (June 2013) ○ All access to CCTV footage is recorded in the School CCTV Access Log

5. Data security: Management Information System access and Data transfer

Strategic and operational practices At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

staff,
governors,
students
parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake regular house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use remote secure back-up for disaster recovery on our network / admin, curriculum servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school gates. They must remain turned off and out of sight until they have exited the school gates. Staff members may use their phones in agreed staff areas and not in the presence of students. Emergency situations will be at the discretion of the Head teacher or named member of SLT. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny

and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. If contact is essential, then permission may be granted and a phone call made in the reception area with staff present or in an agreed staff supervised area.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on personally-owned mobile devices. School phones / digital cameras are to be used for supervised activities where photographs / videos are needed e.g. residentials, trips, extra-curricular activities, visits.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released in accordance with the school policy. (see Appendix A)
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations. Students must adhere to the Examination Code of Conduct in relation to mobile devices which are displayed during examinations. The School Examinations officer will reiterate key messages at strategic times before and during examinations. Students in possession of a mobile device must hand it in before entering the examination hall / examination room.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences in relation to the sharing of numbers, information, images, videos etc.
- The document in the following link contains guidance and information from the Government about sexting in schools

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action will be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video At St Gregory's Catholic High School

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify students in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific student photos are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term use
- The school blocks/filter access to many social networking sites or newsgroups unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix A

Learning Organiser Page

Personal Equipment

No personal electronic entertainment equipment i.e. iwatch etc. are allowed in school

Mobile Phones

We strongly advise that mobile phones **should not** be brought into school. If, for a specific safety reason they are brought in, they must be **turned off** (not placed on silent) and stored **out of sight** (bags/lockers) on arrival at the school gates. They must remain off and out of sight until you have exited the school gates.

If your phone is seen/used in school, it will be **confiscated and stored overnight** in a safe place; a parental signature is required for its return, the following day at 3 p.m.

Following a second confiscation, parents/carer must collect their child's phone.

Use of phones whilst on school premises is a serious breach of our Safeguarding rules and will result in parental contact and resulting sanctions.

Bicycles must be put in the bike racks provided. School insurance does not cover theft of, or damage to, bicycles so you need to be very conscious of security as well as safety if you cycle to school. Bikes must be walked on and off school premises to avoid accidents.

Lost Property

Inform your Form Tutor immediately. Hand in found items to Reception/ Pastoral Office.

The school accepts no responsibility for monies or valuables brought into school.

All policies are available on the school website.