Gunnersbury Catholic School

Online Safety Policy

Created: July 2021
Implemented: September 2021
Review: July 2022

Governing Body Committee: Welfare Committee
Chair of Governors: Andrew Flatt

GUNNERSBURY CATHOLIC SCHOOL .....

Contents

Version Control

As part of the maintenance involved with ensuring our e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Gunnersbury Catholic School Online Safety Policy
Date	July 2021
Author	C Mahon
Approved by head teacher	July 2022
Approved by Governing Body	
Next Review Date	July 2021

Introduction and Overview

Rationale and Scope

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Gunnersbury Catholic School withrespect to the use of ICT-based technologies.
- safeguard and protect the students and staff.
- assist school staff working with students to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- have clear structures to deal with online abuse such as online bullying 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 but not limited to, online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, gambling.
- lifestyle websites, for example pro-anorexia / self-harm / suicide sites
- hate content
- content validation: how to check authenticity and accuracy of online content
- students working from home unsupervised and staff working from home for extended periods of time.

Contact

- grooming (sexual exploitation, radicalisation etc.)
- online bullying in all forms
- social or commercial identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- aggressive behaviours (bullying)
- 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) of Youth Produced Sexual Imagery
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

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

The Education and Inspections Act 2006 empowers Headteachers / Principals 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 online bullying, or other online 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. In the case of both acts, action can only be taken over issues covered by our published Behaviour for Learning Policy.

Gunnersbury Catholic 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 online safety behaviour thattake place out of school.

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and Hounslow Safeguarding Children Partnership guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. London Grid for Learning (LGfL) services, CPOMS and Impero • To be responsible for ensuring that staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' undertaken so the curriculum meets need of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator during the safeguarding updates. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager) • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety, i.e. through the welfare governors committee. • To ensure the school's website includes relevant information

Role	Key Responsibilities
Online Safety Co-ordinator / Designated Child Safeguarding Officer	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • promotes an awareness and commitment to online safety throughout the school community • ensures that online safety education is embedded across the curriculum • liaises with school ICT technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident by the safeguarding admin assistant using data from CPOMS and Impero. • facilitates training and advice for all staff • oversee any student surveys / student feedback on online safety issues • liaises with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns
Governors / Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator / Officer (including online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly
Network Manager/technician	• To report any online safety related issues that come to their attention, to the Online Safety coordinator. • To manage the school's computer systems, ensuring: • School password policy is strictly adhered to • Systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) • The school's policy on web filtering is applied and updated on a regular basis

Role	Key Responsibilities
	• That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy, and understand any updates annually. The AUP is signed by new staff on induction • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To ensure that any remote access to School software is only ever done from personal laptops or tablets which are password protected and are solely used by that staff member and not shared with any family member or friend • To never share their login information and passwords and to report any suspected misuse of their personal devices and access data • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social media etc. • At the end of the period of employment / volunteering to return and equipment or devices loaned by the school. This will include Usernames and passwords, PINs and to allow devices to be reset or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Students	• Read, understand, sign and adhere to the Student / Student Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials and never share their login information or passwords • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on online bullying. • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of online safety policies • to contribute to any 'pupil voice' / survey that gathers information of their online experiences
Parents/carers	• to monitor their child's use of IT when they are working from home and to ensure that they are logged onto their lessons during any periods of remote learning • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school's Student Acceptable Use Agreement with their children • to access the school website / on-line student / student records in Progresso in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups including Parent groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology

Communication:

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

- Policy to be posted on the school website/ Staff shared file
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all 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 planners and master personnel record

Handling incidents:

- The school will take all reasonable precautions to ensure online 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 as well as guidance on how to report incidents. Reference in the incident logging template
- Online Safety Coordinator acts as first point of contact for any incident
- Any suspected online risk or infringement is reported to the Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer)

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy)

- The school has ICT strategic group who will be responsible for document ownership, review and updates in liaison with the Child Protection Lead
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the school Online Safety Co-ordinator with whole school consultation. It 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 Online Safety policy will be disseminated in detail to all members of staff and students

Education and Curriculum

Student online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL online safeguarding and national guidance. 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.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through the Student Acceptable Use Policy which is signed by students and parents in their planner. Students are to be reminded of this by Computing/ICT teachers/tutors/HOY
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons such as ensuring that when using projectors in class all other software (email etc) is closed so there isno possibility of sensitive information being inadvertently shared with students.
- 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;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection – LGFL USO_FX2 system (http://my.uso.im/) AND Secure Access (https://sa.education.gov.uk/idp/Authn/UserPassword);
- Makes regular training available to staff on online safety issues and the school's online safety education program; annual September induction for all staff and regular updates through whole staff training sessions and regular TED talks.
- 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 Online Safety policy and the school's Acceptable Use Policies. DSL to undertake relevant training as appropriate.

Parent awareness and training

Gunnersbury will provide online safety and guidance for all parents/guardians

Expected Conduct and Incident management

Expected conduct

In this 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 online safety practice when using digital technologies in and out of school and realise that the school's Online Safety Policy covers their actions in and out of 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 online bullying

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Know to take professional, reasonable precautions when working with students, previewing websites before use
- are responsible for reading the school's online safety policy and using the school IT systems accordingly, including the use of mobile phones, and hand held devices.
- Must ensure that all digital resources used in the school have the appropriate license or copyright agreement before use

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 students to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the online 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
- incidents reported from the Impero-safe system are logged and action taken as appropriate and inline with the school's policies
- any child protection issues or contravention of acceptable use are dealt with in accordance with child protection/safeguarding procedures. Evidence is recorded and logged and senior leaders of the school notified immediately.
- 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 (e.g. the Local Authority (LA) and LGFL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police and Internet Watch Foundation (IWF) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed / audited and reported to the school's senior leaders including the Governors' Welfare Committee and Full Governing Body
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school

- Accepts that Filtering and monitoring systems are only ever tools in helping to safeguard children when online and this school has an obligation to "consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum."
- Informs all users that all IT use including internet / email use is monitored
- Has the educational filtered secure broadband connectivity through the LGfL (Regional Broadband Consortium)
- Uses Impero e-safe to monitor all IT use on all school owned devices, monitoring onsite and offsite activity
- Uses the LGfL Web Screen filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. The filtering system is appropriate and in line with DFE and UK Safer Internet Centre guidance. All changes to the filtering policy are 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 staff and the age appropriate expectations of pupils.
- Ensures network health through use of Sophos anti-virus software (from LGfL) etc.
- Uses DfE, LA or LGfL approved systems such as S2S, LGFL USO FX2, secured email to send 'protect-level' (sensitive personal) data over the Internet
- Blocks all Chat rooms (expect Google) and social networking sites except those that are part of an educational network orapproved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protects students;
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- 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: the school's learning platform and school approved platforms
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites is vigilant when conducting 'raw' image search with students e.g. Google image search;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager. Our Network Manager logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' monitoring tools for viewing users applications and Internet web sites, where useful (in all IT suites);
- Has additional local network auditing software installed (System Centre Configuration Manager);
- Ensures the Network Manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies
- Has daily backup of school data
- Uses secure, Microsoft Azure cloud storage for remote data backup. Online backups are always encrypted
- Storage of all data within the school will conform to the GDPR requirements

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network where necessary;
- Staff access to the schools' management information system is controlled through a separate means of authentication for data security purposes;
- We provide students with an individual network log-in username. From Year 7 they are also expected to use a personal password;
- All students have their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account;
- Access to the School's network and software is removed for all leavers in accordance with GDPR requirements
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day to save energy.;

- Acknowledges that data protection is key in schools and, as more teachers have access to high level pupil information through access to Schools MIS systems, and requires staff to ensure their computer is locked or logged off when not in use.
- Has blocked access to music / media download or shopping sites – except those approved for educational purposes; (same as point 10 on page 16)
- Ensures all equipment owned by the school or connected to the network has up to date virus protection
- Makes 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;
- Makes clear that staff are responsible for ensuring that any device 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" as defined by HM Revenue & Customs.
- Makes clear that staff must not access any system remotely or online which contains or allows the download of any staff related records, on any device which is not owned by the school. This includes HR, Payroll and spreadsheets which contain staff records. Student and parent information which is highly confidential e.g. Health Records and Vulnerablechild records are also classified as highly sensitive.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Keeps an asset log of all equipment including equipment allocated to individuals.
- Has integrated curriculum and administration networks, but access to the staff Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school / LA approved systems: staff can access the Student Shared Area where only student resources are located
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited and restricted and is only through approved systems;
  e.g. technical support or MIS Support
- Provides students and staff with access to content and resources through Google Classroom which staff and students access using their username and password (their USO username and password);
- Has a clear disaster recovery system in place for critical data that includes a secure, remote offsite back up of data
- Uses secure data transfer, the DfE secure s2s website for all CTF files sent to other schools and the LA;
- Ensures 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 FX2) – nominated staff only;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;

- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and students must always keep their password private, must not share it with others. They must also not allow another user to user their own account on any devices or system. They will notify the school if they suspect their account has been compromised.
- Usernames and passwords are unique to each pupil at an appropriate level of complexity for the age range.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords. Strong Passwords are at least seven characters and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols. https://www.cyberaware.gov.uk/passwords
- We require staff to change their passwords into the MIS, LGfL USO admin site each year

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of students or staff on the school website. We do not publish student emails, but we do publish staff school email address. Class email addresses can only receive emails from staff email addresses.
- 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 e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Students:

- Students should only receive external mail from, and send external mail to acceptable addresses
- 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 e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of 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 and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

- Students sign the school Agreement Form to say they have read and understood the online 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
- Staff will use the school email systems for professional purposes only
- Staff will ensure that any remote access to School software is only ever done from personal laptops or tablets which are password protected and are solely used by that staff member and not shared with any family member or friend
- Staff will never share their login information and passwords and will report any suspected misuse of their personal devices and access data
- Never use email to transfer staff or student personal data. 'Protect-Level' data should never be transferred by email. Staff must use secure, LA / DfE approved systems to transfer 'Protect-Level' data. These include: S2S (for school to school transfer); Collect; USO-FX2
- 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 our school Agreement Form AUP 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.

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
- Photographs published on the web do not have full names attached;
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them

Learning platform

- Our school learning platform utilises Google Classroom
- Uploading of information on the schools' online learning space 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 school's online 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 Platform;

Social networking

- Staff are instructed to always keep professional and private communication separate.
- 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.
- Students are taught to use forums, walls and messaging through Google Classroom to teach them how to usesocial media 'type' applications responsibly.
- The school's preferred system for social networking (externally, only through approved Twitter accounts) will be maintained in adherence with the communications policy.

School staff will ensure that in private use

- No reference should be made in social media to students, parents / carers or school staff
- School staff should not be online friends with any student. Any exception must be approved by the Headteacher
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- Students are required to sign and follow our student acceptable use agreement

Parents

- Parents are reminded about social networking risks and protocols through our parental acceptable use agreement and additional communications materials when required
- Are reminded that they need to ask permission before uploading photographs, video or any other information about other people

Video Conferencing

This school

- Uses Zoom for video conferences
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without permission except where disclosed to the Police as part of an investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Equipment and Digital Content

Currently the school WiFi setup for all users is on the same network.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Year 7-11 students are not allowed to bring mobile phones into school Years 12 and 13 students' mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staffmembers may use their phones during school break times and away from students.
- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- In line with current legislation (The Education Act 2011) 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 system. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seekspecific permissions to use their phone at other than their break times.
- 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.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobilephones or mobile devices.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School does not allow mobile phones to be brought into school by years 7-11.
- 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 in the student services office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- 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.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised, if necessary, to contact their child via the school office
- Students should protect their phone numbers by only giving them to trusted friends and family members. 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.

Staff use of personal devices

- 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, unless agreed with the Headteacher.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- 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 - school owned equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may 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 doesn't 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

In this 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 son/daughter joins the school;
- We do not identify students in online photographic materials or include the full names of students 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 students; (staff are able to take photos/videos on their phones only with the permission of the DSL
- Images should not be left on school owned devices or memory cards. Images should be stored on the school central areas and securely deleted if no longer required.
- If specific student photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their online 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 identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data private and what to do if they are subject to bullying or abuse.

Appendices

Acceptable Use Policies and Agreement

Gunnersbury Catholic School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies tosupport their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe andto be fair to others.

Parents Acceptable Use Agreement

The ICT facilities are owned by the school and their use is an entitlement for all pupils subject to the conditions detailed here. Pupils wishing to use the resources must sign this statement (countersigned by a parent or guardian) and return to the school.

General Conditions:

- All ICT-based activity must be appropriate to a school environment.
- Use of the School's facilities for personal financial gain, gambling or advertising is forbidden.
- Copyright of materials must be respected. If in doubt, check first.
- Access must be made to the ICT resources only via the user's authorised account and password, which must not be made available to any other person.
- Activity or vandalism that threatens the integrity of the school's facilities, or activity which corrupts other systems is forbidden.
- The School reserves the right to monitor the use of ICT resources at any time.
- The School reserves the right to examine or delete any files held on its resources and to monitor both files held and Internet sites visited.
- Without express permission, users may not knowingly install software (applications, programs, plug-ins, cookies etc) on any computer or delete, update, corrupt or otherwise alter existing software.
- Users may not attempt to access any ICT resources to which their authorised username does not give access.

Email Conditions:

- Students must only use the Gmail account linked to their Google Classroom login.
- Email messages should be sent only to staff members.
- Email messages must be appropriate to a school environment. The sending of anonymous, threatening, abusive or embarrassing messages and the forwarding of chain letters is forbidden.
- Emails sent by students on official school business to external agencies (e.g. to request information on a project) must be approved by the member of staff responsible before being sent.
- Without express permission, email attachments must not be opened. Attachments for the transmission of school work between home and school are exempt from this restriction.

Internet Conditions:

- Use of the Internet to access inappropriate materials is forbidden.

Please note: In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. It is not possible, however, to guarantee that particular types of material will never appear on a terminal, given the international scale and linked nature of information stored on the Internet.

- The school cannot accept liability for any such materials accessed, or any consequences thereof.
- Without express permission, chat services, or Internet Relay Chat (IRC) channels or other forms of instant messaging systems or apps may not be accessed.
- Without express permission, files must not be down loaded from the Internet.
- Information which could identify the user or any other person directly must not be published on any Web page.

Failure to comply with the requirements of this statement may result in the temporary or permanent loss of access rights, it should also be noted that the use of a computer system for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. The school will consider permanent exclusion for serious breaches of this code.

Pupil's name: _____

Signature of Parent/Guardian: _____ **Date:** _____

The use of digital images and video

To comply with GDPR, we need your permission before we can photograph or make recordings of your son/daughter.

Gunnersbury Catholic School rules for any external use of digital images are:

If the student is named, we avoid using their photograph.If their photograph is used, we avoid naming the student.

Where showcasing examples of students work or achievements we only use their first name, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film.

Only images of students in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your son/daughter being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made of students in music or drama, as part of the learning record, and then sharing with their parent / guardian.

- Your son/daughter's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your son/daughter's image being used in a presentation about the school and its work in order to share its goodpractice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your son/daughter's picture could appear in the media if a newspaper photographer or television filmcrew attends an event.
Note: If we, or you, actually wanted your son/daughter's image linked to their name we would contact you separately for permission, e.g. if your son/daughter won a national competition and wanted to be named in local or government literature.

The use of social networking and online media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site and/or police where appropriate.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

Student Acceptable Use Policy

Online Safety Agreement & Acceptable Use of ICT & Social Media

Gunnersbury Catholic School has a curriculum computer network which full internet access to assist learning. Students canuse this facility only when parents/guardians have signed this agreement.

Digital Wisdom:
If you receive abusive messages, keep them. You do not have to read them. When the time comes for action they can be used as evidence. If you receive abusive message ask for help from parents/carer, your Form Tutor, Head ofYear, Director of Key Stage or any member of staff. You can also contact your mobile phone provider. Remember: by forwarding a text, email, photo, video, etc, you may be making the problem worse. You could be unwittingly involving yourself in bullying. You may even be breaking the law.

I agree to:

1. I will keep my login and password details secret and will not access anyone else's files.
2. I will only use the computers for schoolwork and homework.
3. I will not bring files into school that can harm the school network or be used to compromise school security tools.
4. I will only use the internet for appropriate educational purposes.
5. I will not use messaging software or clients.
6. I will use polite standard English in all communications and good email etiquette at all times. Such as: Dear, Thank you, Please, etc.
7. I will not give my personal information that could be used to identify me, my family or friends on any space, unless a trusted adult has given me permission or reviewed the site.
8. I understand that my files will be checked and that my use of the internet will be monitored.
9. I understand that the use of all school devices is monitored inside and outside of the school including use at home. Any activity which is considered to contravene this agreement or may be considered to fall within the schools safeguarding requirements is automatically reported to the school.
10. I will not undertake any activity. including loading software, that is found to threaten the integrity of the computer network or attacks or corrupts other systems.
11. I will respect the copyright of materials.
12. I will not use any digital device to access, post or produce anonymous messages; material of an inappropriate, threatening, discriminatory, racist, homophobic or offensive nature. I will not post derogatoryor negative comments about the school or any member of the school community.
13. I will not post/upload on the internet or social network any materials which can cause damage to my personal reputation, other people's reputation or the reputation of the school.
14. I will not post or upload any materials or photos which can identify the school and breach the safety of students on any social networks such as Youtube/Facebook/msn/Ask
15. FM/Twitter/Snapchat/Instagram/WhatsApp/. I will respect the required age to create accounts on social networks.
16. I will follow all the guidance provided by school on the safe use of my laptop/tablet and take care of my school laptop/tablet and protect it from damage. I understand that insurance cover is limited.

17. I will respect the school computer hardware and not abuse it.
18. I will report to a member of staff, any videos or materials, showing the school buildings or students in uniform, posted on the web without the school's permission.
19. Breaching any of the above will be subject to an appropriate sanction, which may result in withdrawal of Internet access in school and ultimately in an exclusion.
20. In line with the Social Media Policy, we reserve the right to look at the students' mobile phones and laptops when conducting investigations
21. I will never arrange to meet someone I have only ever previously met on the internet, by email or in a chat room, unless it take a trusted adult.
22. If I see anything I am unhappy with or receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

Student's Signature …….. Date …….

As the parent/carer of the student signing above, I grant permission for my son/daughter to use email and the internet. Iunderstand that students will be held accountable for their actions. I also understand that some materials on the internet may be objectionable and I accept joint responsibility for the setting of standards for my son/daughter to followwhen selecting, sharing and exploring information and media. I will also check her mobile devices on a regular basis to ensure her safety and will make sure appropriate filters are in place at home.

Parent/Carer's Signature …….. Date …….

Acceptable Use Policy Staff / Volunteer / Contractors / Governors

Name of School	**Gunnersbury Catholic School**
AUP review Date	**July 2021**
Date of next Review	**July 2022**
Who reviewed this AUP?	**C Mahon**

Acceptable Use Agreement: All Staff, Volunteers, Contractors and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.

Gunnersbury Catholic School regularly reviews and updates all AUA documents to ensure that they are consistent with theschool Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone or let any other individual knowingly use my account(s).
- When working remotely, I will only access the School's software (ie email or Progresso) from a personal laptop or tablet which is password protected and is solely used by me and not shared with any family member or friend.
- I will never access the School's software from a public device
- I will follow school procedures in the creation and use of my password (must not contain any part of your username or full name, must contain characters from 3 of the following 4: upper case (A-Z), lower case (A-Z), numbers (0-9), symbols e.g. £,!,*). If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will only use the approved email system, Learning Platform and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager, ICO and / or Online Safety Co-ordinator.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- Any data and material brought onto the school site and / or onto the school network must be appropriate for the school environment. The Headteacher and / or authorised staff have the right to view all data without consent.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's anti-virus and other e-safe systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will not take into classrooms / only use in staff areas.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc., will not identify students by name, or other personal information.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and details of these are given to the ICT Strategy Group.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the Learning Platform and follow data protection protocols to interact with them.

- I will ensure any confidential data and data categorised as 'Protect-Level' is never removed or accessed from a device not owned by the school and is never transferred onto a personal USB stick on memory card.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the Child Protection lead / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Headteacher and / or Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that all activity on all school owned devices is monitored by Impero and is active inside and outside of the school network.
- I will only use any LA system I have access to in accordance with their policies.
- *Staff that have a teaching role:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Staff Acceptable User Agreement

User Signature

I agree to abide by all the points in the Acceptable Use Policy.

I understand that I have a responsibility for my own and others safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school'smost recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature _____ Date _____

Full Name _____ (printed)

Job title _____

Authorised Signature (Headteacher)

I approve this user to be set-up on the school systems relevant to their role

Signature _____ Date _____

Full Name _____ (printed)

To be filed in staff personnel records for future reference

Roles and Definitions

Roles

Role	Staff
Headteacher	K Burke
SIRO (Senior Information Risk Officer)	K Smith
Online Safety Co-ordinator	C Mahon
Designated Safeguarding Officer Lead	C Mahon
Network Manager	S Thomas
IT Technical Staff	S Thomas
Safeguarding Governor	Linda Pope
Online Safety Governor	Linda Pope
Computing Curriculum Leader	P Kilgarriff
Learning Platform Leader	N Quinn
LGFL Nominated Contacts	K-A Smith
Chair of Governors	A Flatt
ICT strategic group	S Thomas, K Smith, K Burke, C Mahon, P Kilgarriff

Ordered as first referenced in policy document

Online Incident Log

Details of ALL online safety incidents to be recorded by the Online Safety Co-ordinator. This incident will be monitored by the Headteacher, SLT, Online Safety Governor or Safeguarding Governor.

Date & Time	Name of Student or Staff member	Room & Computer / Device name	Details of incident (Including evidence	Actions	Name and roll of person completing this entry

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for Investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

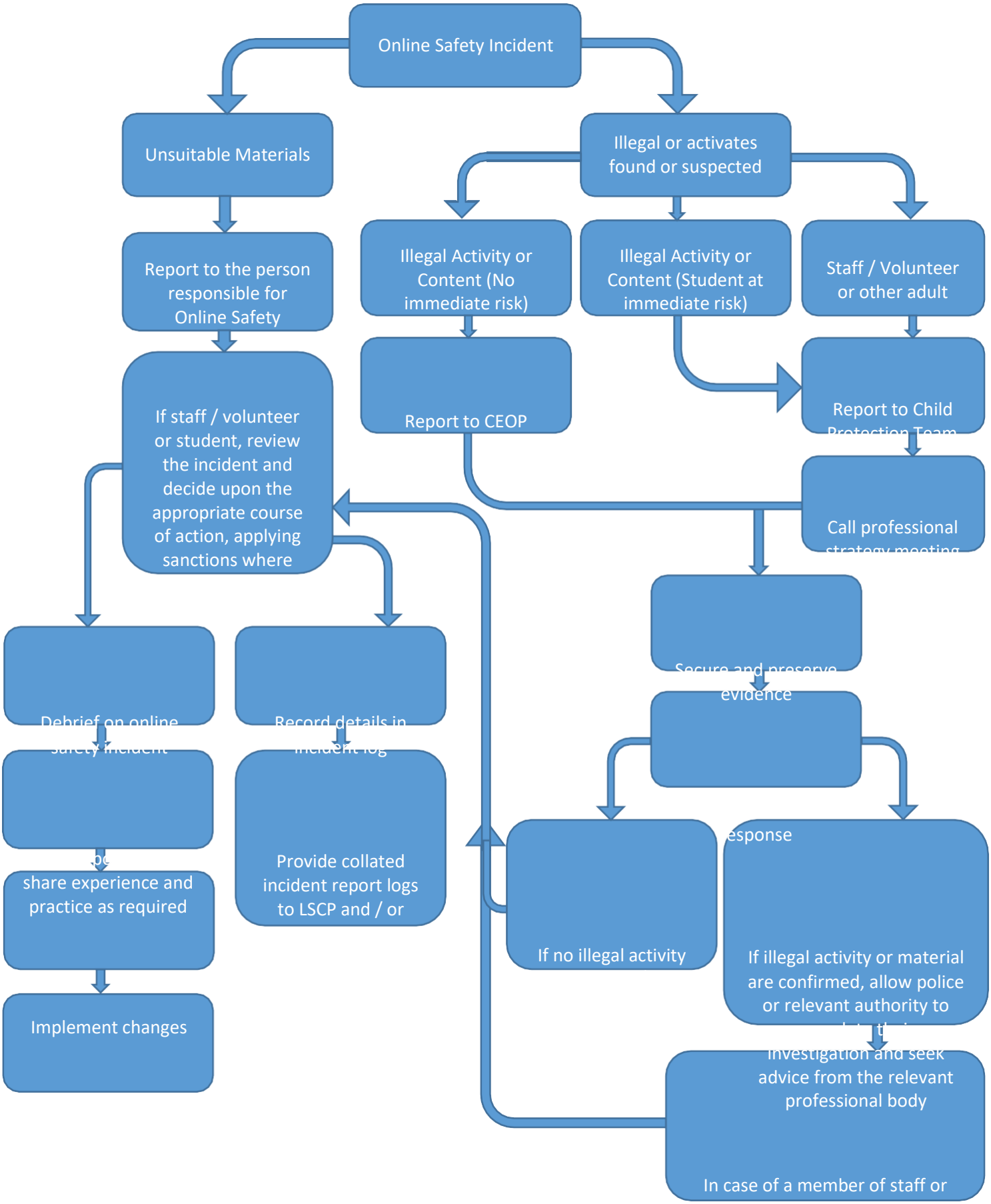
Name	
Position	
Signature	

Name and location of computer used for review (for website)

Website(s) address / device	Reason for concern

Conclusion	Action proposed or taken

Online Safety Incident Flowchart



Online-Safety Policy Infringement Document

Name of School	**Gunnersbury Catholic School**

Policy: How will infringements be handled?
Whenever a student or staff member infringes the Online-Safety Policy, at school or through online learning at home, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.
The following are provided as **exemplification** only:

STUDENT	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email and communications tools • Unauthorised use of mobile phone/personal device in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email and communication tools after being warned • Continued unauthorised use of mobile phone/personal device after being warned • Continued use of unauthorised instant messaging / social networking sites, Games sites • Use of Filesharing software e.g. BitTorrent, for illegal downloading • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not notifying a member of staff of it	**Refer to Class teacher/ Head of Department / Year tutor / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

STUDENT	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Transmission of commercial or advertising material • Use of systems to circumvent schools online-safety tools such as VPN and proxy sites	**Refer to Class teacher / Year Tutor / Online-Safety Coordinator / Head teacher / removal of Internet and/or online services access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
• Continued sending of emails or messages regarded as harassment or of a bullying nature Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent Sharing or requesting of images or content of a minor that would be considered sexual or inappropriate. • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the service provider if appropriate. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, social networking etc. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Lack of due care resulting in infection or distribution of viruses or malware • Misuse of first level data security, e.g. sharing of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	**Referred to Head teacher / Governors; Other safeguarding actions:** ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. ▪ Identify the precise details of the material. *Escalate to LA /LSCB, Personnel/ Human Resources.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on online-safety issues, (see LGfL safety site).

Useful Online Safety Links

Digitally Confident
www.digitallyconfident.org

LGfL
www.lgfl.net/services/london-mail

Childnet
www.childnet.com

Thinkyouknow
www.thinkyouknow.co.uk

Internet Watch Foundation
www.iwf.org.uk

CEOP
http://ceop.police.uk

Beat Bullying
www.beatbullying.org/gb/who-is-on-this-site

Reporting links for popular online services
http://cyberbullying.us/report

Guidelines on prosecuting cases involving communications sent via social media
www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media

Dealing with indecent images of children in the workplace: A Best Practice Guide
www.iwf.org.uk/resources/best-practice-guide

How to report and handle a security incident

What is a security incident?

A security incident can occur when our policy on information security and communication is not followed. If our policy is not followed, the security of our information is put at risk. This can happen because people do not understand the security requirements, do not take care, or choose deliberately not to follow the policy. There are some examples below, although it is not a full list.

- Suspecting your email and/or login details have been compromised
- Using, or being asked to use, another person's login or password (or both)
- Not locking your PC before leaving it, if you are logged in
- Allowing confidential information to be passed on to people who do not have the correct authorisation to see it or not preventing this
- Stolen or lost electronic equipment, including laptops
- Viewing or downloading material which is illegal or banned by other regulations or rules
- Sending abusive emails, or forwarding racist or sexist jokes or emails
- Allowing someone to enter the building without an appropriate pass (where applicable)
- Computer viruses

Employees

Employees must immediately report all incidents, even those they think are minor, to their manager or, if he/she is unavailable or personally involved in the incident, to the Headteacher or Chair of Governors. Employees may be asked to provide information to help any investigation that may follow.

Managers who receive a report of a security incident

- All incidents where information has been lost or stolen must be notified to senior management within the school.
- If there is enough evidence to justify a formal investigation under the School's disciplinary procedure, they must follow the procedure laid down in the disciplinary procedures.
- With support from their Headteacher, managers must take any necessary action within their area of responsibility to prevent further risk to our information or to limit the impact of the loss of or damage to our information from the reported incident.
- With support from their Headteacher, managers must also take any necessary action within their area of responsibility to prevent similar incidents occurring in the future.
- All reported incidents must be promptly logged and the relevant staff must ensure they are thoroughly investigated. The log should include an incident number where the police have become involved in the incident.
- A risk assessment should be carried out to ascertain whether this security incident should be reported to the Information Commissioners Office. To assist in this procedure a sample risk assessment can be found in on the proceeding pages.
- The Headteacher and other relevant people in the School will work to ensure that any necessary action is taken to prevent similar incidents occurring in the future.

Security Incident Report

Incident Date		Incident Number	
Incident Type			
Police incident number (where applicable):			
Personnel involved			
Description of event:			
Chronology of events			
Date	Details – Please use a separate sheet if you need additional space.		
Where appropriate, have those affected been informed?		Yes ☐	No ☐
Lessons learned:			
Recommendations:			
Do I need to inform the Information Commissioners Office?		Yes ☐	No ☐
Name of staff member responsible for investigation:		Senior Team aware?	Yes ☐ No ☐
Signed:		Date	

GUNNERSBURY CATHOLIC SCHOOL

Smile and stay safe

Staying safe means keeping your personal details private such as: full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

SAFETY ONLINE