Gunnersbury Catholic School

E-Safety

and

Data Security policy

Version date: September 2020

Review date: August 2021

Gunnersbury Catholic School

POLICY 2020-2021

1. Aim

As part of the curriculum entitlement, students study computing across the key stages. This comprises of three main strands: digital literacy, computer science and information technology. It is the latter and its use at Gunnersbury Catholic School that provides the focus in this policy.

Given the rapid advance of technology in today's society, we hope all pupils can:

- Understand and apply the fundamental principles of computing
- Analyse problems in computational terms, gain practical experience of writing computer programs
- Evaluate, apply and be creative with information technology, including new or emerging technologies using IT confidently and responsibly

We will support this by:

- Ensuring all pupils reach the highest possible levels of achievement
- Enabling pupils to become independent users of IT, and benefit from the IT resources, tools and its impact on society
- Teaching pupils good Health and Safety attitudes and practice

IT includes any hardware or software for users to electronically communicate or handle data or information.

Health and Safety

All activities, whether in school or off site, will be guided by the school's Health and Safety and E-safety policies. Where necessary, individual Data Protection Impact Assessments (DPIAs) will be put into place to ensure the safety of pupils and the integrity of the school IT system. All equipment is PAT tested annually.

E-safety refers to all technologies and electronic communications and the need to educate young people and staff about the online benefits and risks both within and outside of the College. E-safety is within the scope of other policies including Keeping Children Safe in Education, Student Behaviour, Child protection, Bullying, Curriculum and Health & Safety.

Copyright and Licensing

All software and hardware used on the school's system should be correctly licensed. All staff and students should sign an agreement of acceptable use

1. Principles and Values

Gunnersbury Catholic School holds personal data on students, staff and other people to help conduct day-to-day activities. Its loss can result in a data breach by illegal activity to cause harm to individuals, groups or the reputation of the school.

Everybody at Gunnersbury's has a shared responsibility to secure any sensitive information in line with the General Data Protection Regulation 2018.

The school has key staff overseeing E-safety consisting of the Designated Safeguarding Lead (C. Mahon) and the ICT Manager (S. Thomas).

E-safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and students through education and policies.
- Sound implementation of E-safety practice in both administration and curriculum

2. Teaching and learning

2.1 Internet use will enhance and extend learning

Benefits of using the Internet in education include:

- Students' access to learning wherever and whenever convenient.
- Impact teachers' pedagogy through classroom practice and professional development for all staff.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates along with appropriate filtering.
- Exchange of curriculum and administration data with the Local Authority and DfE.

2.2 Students will be taught how to evaluate Internet content

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the ICT Manager.
- Gunnersbury Catholic School will strive to ensure that the use of internet derived materials by students and staff complies with copyright law and is free from plagiarism.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.

2.3 SEND Students

Gunnersbury Catholic School endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the school's e-safety rules.

However, staff are aware that some students may require differentiated teaching or events where, for example, SEND students have poor social understanding and careful consideration is given to group interactions when raising awareness of e-safety.

3. Managing Internet Access

3.1 Authorised Internet Access

- Gunnersbury School will maintain a current record of all staff and students who are granted internet access.
- All staff must read and sign the 'Acceptable IT Use Agreement' before using any school IT resources.
- Parents will be informed that students have supervised Internet access and sign paper or electronic consent form for this purpose.
- Students must apply for Internet access individually by agreeing to comply with the responsible Internet use statement.
- E-safety matters are referred to the Designated Safeguarding Lead or the ICT Manager, if required.

3.2 E-mail

- Students may only use approved E-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive E-mail.
- Students must not reveal personal details of themselves or others in E-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal E-mail accounts may be blocked.
- The sharing of 'viral', social media or mass audience messages with e-mail distribution lists is not permitted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

3.3 Social Networking

- Gunnersbury Catholic School will filter access to social networking sites (except Google Classroom) unless there is a specific and approved need.
- Students should be advised not to disclose personal details e.g. photos of anyone connected with the school.
- Students should be advised on security, set complex passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students should be aware of privacy settings and controls for accounts.

3.4 Managing Emerging and Existing Technologies

Emerging or existing technologies will be examined for educational benefit and a Data Protection Impact Assessment (DPIA) will be carried out before use in school is allowed:

- Mobile phones, games consoles, or other web-enabled devices will not be used for personal use during lessons or formal school time unless a DPIA is approved.
- The sending of abusive or inappropriate electronic communication is forbidden.
- contact@gunnersbury'hounslow.sch.uk is the chosen method of electronic communication with parents.
- Staff have access to a school phone within their department base where contact with students is required.

3.5 Published Content and the College Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff's or students' personal information will not be published.

- The Head teacher will assign a member of SLT to take overall editorial responsibility and ensure that the content is accurate and appropriate.

3.6 Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website.
- Work can only be published with the permission of the student and parents.

3.7 Protecting Personal Data and Preventing Breaches

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

- The school gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of staff and students to keep passwords secure. No user ID or accounts should be shared.
- Staff are aware of their responsibility with any form of personal or sensitive data when accessing school data in terms of who has access to it, who it is shared with and the length of time data is stored.
- A breach of GDPR by the Information Commissioner's Office is defined as "likely to result in a high risk of adversely affecting individuals' rights and freedoms".
    - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- Staff must report any GDPR breach that has the potential to cause personal or reputational harm to any individual, group or to Gunnersbury Catholic School. This must be reported to Mrs Smith in the first instance, who will then decide whether this needs to be referred to the School's Data Protection Officer.

A breach or suspected breach of policy by an employee, contractor or student may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual(s).

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the GDPR;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the GDPR;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern.

3.8 Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. flash or external hard drive) must be checked for any viruses. Users should allow regular virus updates to occur and contact IT support provider immediately if any matters arise. Home computers must have regular system and anti-virus updates to protect both users at home and the school from malicious software.

3.9 Remote Access

- All users are responsible for all activity via remote access facility and ensure access information is both secure and at an appropriate level of security.
- Ensure passwords meet high complexity requirements such as at least eight characters, a combination of letters, numbers, upper/lower case and special characters.
- Protect school information and data at all times, within and outside of the school, including any printed material produced while using the remote access facility.

3.10 Personal Devices (including mobile phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Students are not allowed to bring personal mobile devices/phones to College unless prior agreement was sought; However if they do then they must be switched off and not used at all during school hours.
- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. For example, sixth form students my use their mobile devices in lesson where permitted, with prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

4. Policy Decisions

4.1 Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material and cannot guarantee that unsuitable material will never appear on a school computer. Gunnersbury Catholic School cannot accept liability for the material accessed, or any consequences of Internet access.

The school will exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use is taking place.

4.2 Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by the Designated Safeguarding Lead or member of the SLT, as appropriate.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Students and parents will be informed of the complaints procedure.

5. Communication of Policy

- Gunnersbury Catholic School IT Policy will be available to parents, staff and students on the school website.

Appendices

Acceptable use of ICT Pupils – Appendix A

Letters to parents– Appendix B

Acceptable use of IT Policy for staff, governors and visitors – Appendix C

Acceptable use of Inappropriate Material – Appendix A

Acceptable Use of ICT at Gunnersbury Catholic School Agreement: Pupils

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I am aware that when I take images of pupils and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Mr. C Mahon.

Please return the bottom section of this form which will be kept on record at the school

✂----------

Parent/ carer signature

We have discussed this document with……..(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Gunnersbury Catholic School.

Parent/ Carer Signature: ……..…..

Pupil: …… Form: ……

Date: ……

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are required to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Designated Safeguarding Lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies

User Signature

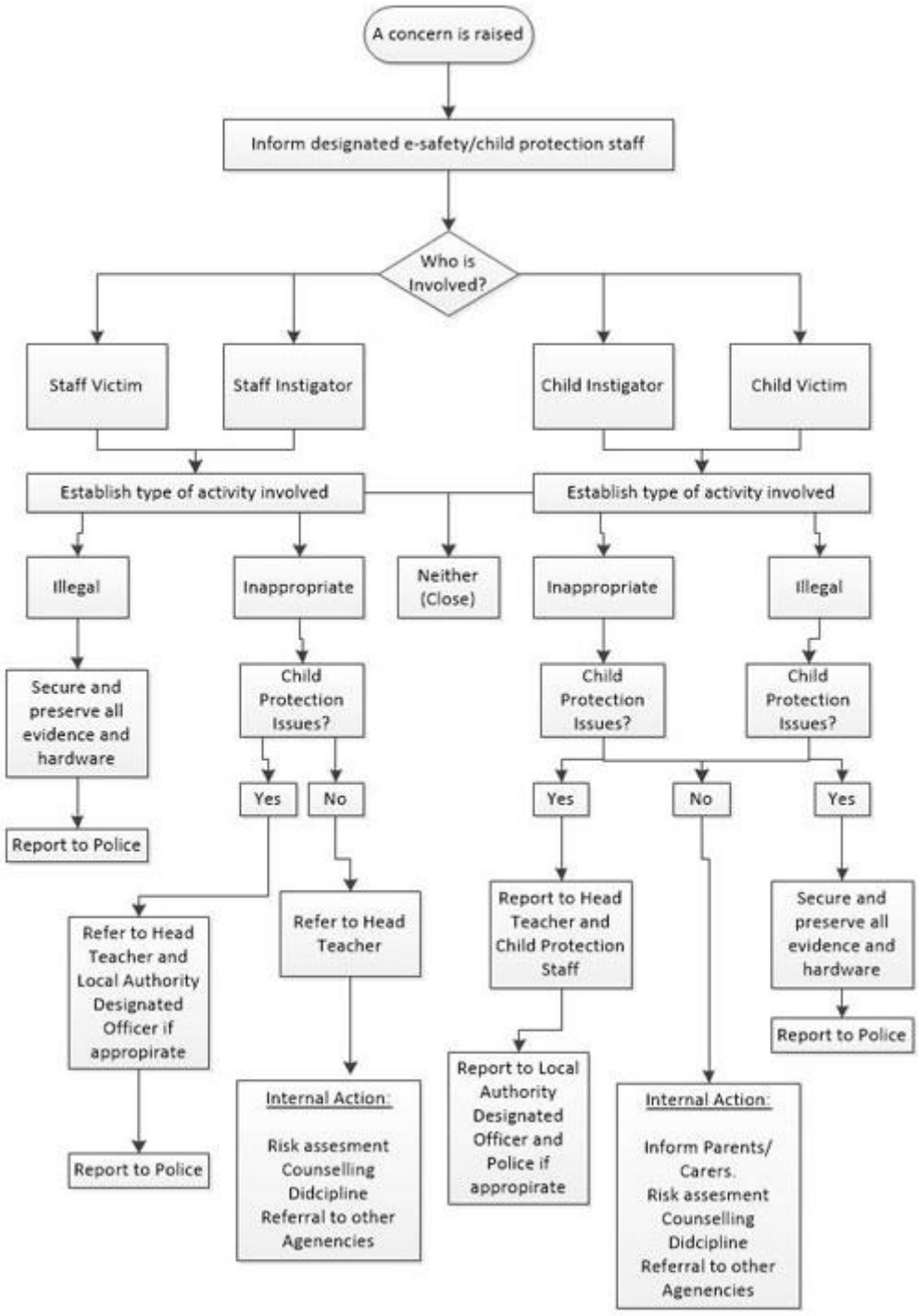
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date: ……

Full Name ……..... *(printed)* Job title: …….

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator, Mr C Mahon,
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Designated Safeguarding Lead. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).


A concern is raised
Inform designated e-safety/child protection staff
Who is Involved?
Staff Victim
Staff Instigator
Child Instigator
Child Victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (Close)
Inappropriate
Illegal
Secure and preserve all evidence and hardware
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
Yes
No
Yes
No
Yes
Refer to Head Teacher and Local Authority Designated Officer if appropirate
Refer to Head Teacher
Report to Head Teacher and Child Protection Staff
Secure and preserve all evidence and hardware
Report to Police
Report to Police
Internal Action:
Risk assesment
Counselling
Didcipline
Referral to other Agenencies
Report to Local Authority Designated Officer and Police if appropirate
Internal Action:
Inform Parents/ Carers.
Risk assesment
Counselling
Didcipline
Referral to other Agenencies

eSafety guidelines are displayed throughout the 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, IM 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