Online Safety Policy

Date Written: April 2023

Next Review Date: April 2025

Table of Contents

Introduction: 3

Curriculum 5

Training 10

Managing ICT Systems and Access 11

Filtering 11

E-Mail 12

Mobile Phones and Devices 12

Pupils Publishing Content Online 13

Staff use of personal devices 14

CCTV 14

General Data Protection (GDPR) and Online Safety 15

Peer on Peer abuse and harassment 16

Appendices 17

Introduction:

The school recognises the substantial benefits new technologies and connectivity offer to our children with huge potential to inspire, create, communicate and learn. However, it is important that our children are protected from and learn how to manage the risks they may encounter in an increasingly connected world. St Gabriel's CofE Academy is committed to educating children about the benefits of the internet, whilst implementing strategies to minimise potential risks to their physical and mental health and wellbeing. The school aims to provide children with the tools to navigate the online, connected world safely, enabling them to detect risk and understand how to seek support.

The school's curriculum aims to meet the Department for Education's statement: *It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.* (Teaching Online Safety in School, 2019, DfE)

The following school policies and procedures should also be referred to

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Whistleblowing Policy
- Preventing Bullying Policy
- Remote Learning Policy
- Acceptable Use of ICT agreement
- Staff Behaviour Policy and Code of Conduct
- Data Protection Policy

The following local/national guidance should also be read in conjunction with this policy:

- Warwickshire County Council Safeguarding Children Guidelines https://www.safeguardingwarwickshire.co.uk/safeguarding-children/i-work-with-children-and-young-people/protecting-children-online
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2023
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children 2023

Curriculum

The school believes the key to developing safe and responsible online behaviour within our school community, lies in effective education. We know the internet and other technologies are embedded in our pupils' lives and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities internet use brings.

To achieve this:

- We provide a curriculum which teaches safety explicitly in Computing, Personal, Social and Health Education (PSHE) and Relationships and Sex Education (RSE).
- We celebrate and promote online safety through our children's experience at school with whole-school activities, including promoting Safer Internet Day each year.
- We discuss, remind and raise relevant online messages with pupils routinely wherever suitable opportunities arise during lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Internet use is carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils are taught how to use a range of age-appropriate online tools in a safe and effective way.
- We remind pupils about their responsibilities through an Acceptable Use Agreement, which every pupil signs and is displayed in classrooms.

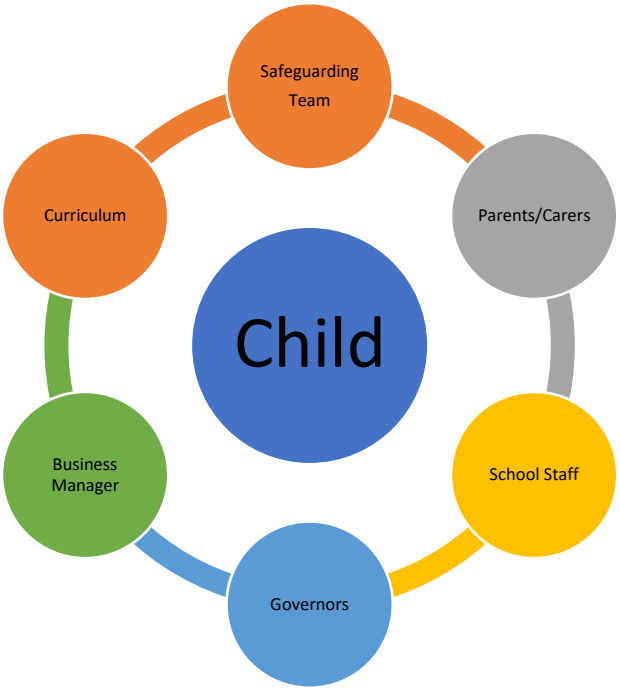
- Staff model safe and responsible behaviour in their own use of technology.
- We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils are guided to use age-appropriate search engines. All use is monitored and pupils are reminded of what to do if they come across unsuitable content.
- Pupils are taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies; parents or carers, teachers or trusted staff members, or organisations such as ChildLine and CEOP.

Remote/Home Learning

We endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and online learning platforms (Seesaw/Tapestry).

We expect pupils to follow the same principles, as outlined in the school's Acceptable Use Agreement, whilst learning at home. Any concerns including inappropriate behaviour occurring on any virtual platform must be recorded and reported via the school's Child Protection Online Management System (CPOMS) to the school's Designated Safeguarding Leaders (DSL/DDSL).

Roles and Responsibilities



Governors are responsible for ensuring:

- The approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- A member of the Governing Body holds responsibility for reporting regularly on Online Safety alongside the nominated Safeguarding Governor.

Safeguarding Team are responsible for:

- Ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles.
- Reviewing any online safety concerns and taking action if appropriate to ensure safety.
- Reviewing outcomes and trends in Online Safety at regular Safeguarding Team meetings.

The Business Manager is responsible for ensuring:

- The school's technical infrastructure is secure, appropriately filtered and protected and any misuse or malicious attacks are reported and responded to promptly.

School Staff are responsible for ensuring:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problems to the relevant staff member:
  - Conduct concerns – Headteacher
  - Safety concerns – DSLs
  - Technical difficulty – Business Manager
- They apply the school's behaviour policy.
- That all digital communications with pupils / parents should be on a professional level and only carried out using official school systems.
- Online safety practice is embedded within the school's curriculum and other activities.
- They help pupils understand the online safety and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities.

Pupils are responsible for:

- Using the school digital technology systems in accordance with the Pupil Acceptable Use agreement.
- Reporting issues, abuse or misuse to a trusted adult.
- Following rules on the use of mobile devices in school.
- Adopting good online safety practice when using digital technologies in and out of school and acknowledge that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and connected devices in an appropriate way. The school will take opportunities to help parents understand these issues through parents' evenings, newsletters, letters, the website and information about national and local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Careful supervision of their child's communication and activity online and on mobile devices.
- Their children's personal devices in the school.
- Digital and video images taken at school events.
- Their modelling on online communication and behaviour.

We ask parents to engage in the timely and meaningful sharing of information about their children's learning and wider school life through emails, social media, the school website and online learning platforms.

Training

Teaching Staff

Staff receive regular information and training on online safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the Online Safety Policy, the school's Acceptable Use Policy and Code of Conduct for All Staff Policy.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate online safety messages and guidance when children are using technology within their lessons.
- All staff understand the potential risks children going online can have and will monitor children's online use in school.

Governors

Governors take part in annual Safeguarding training, which includes online safety. Governors have access to further courses delivered virtually or in person throughout the year, relevant to safeguarding and digital use.

Parents

Parent training is provided through online safety workshops, school produced information and signposting to relevant national and local campaigns and literature.

Managing ICT Systems and Access

- All users will sign an Acceptable Use Agreement provided by the school, appropriate to their age and type of access. Users are made aware that they must take responsibility for their use and behaviour whilst using the school's systems and that such activity is monitored.
- Internet access by pupils has staff supervision when in school.
- Members of staff access the internet on school desktops and laptops using an individual ID and password, which they keep secure. They ensure that they log out after each session and not allow pupils to access the internet through their ID or password.

Filtering

- The school has a filtering system in place which is managed by our IT support company and reports sent twice daily to our School Business Manager. Tagged phrases and websites are identified and blocked.
- All desktop PCs are monitored using IMPERO software which uses keyword detection and digital safeguarding tools to support the school in identifying potential online safeguarding incidents.
- If staff or pupils discover an unsuitable site, it must be reported to the school's Business Manager who will direct the school's IT Consultant to block and remove access.
- If users discover a website with potentially illegal content, this will then be communicated to the school's IT Consultant to block and remove access. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, Child Exploitation and Online Protection Command (CEOP) and the Internet Watch Foundation (IWF).
- Any amendments to the school 'block and allow' lists will be checked and

assessed by the school's IT Consultant in consultation with the Business Manager and Head teacher. Once directed, the school's IT Consultant will make agreed amendments.

- The evaluation of online content materials is a taught across the curriculum.

E-Mail

- Staff should only use approved email accounts allocated to them by the school.
- Staff should not use personal email accounts for professional purposes; especially to exchange any school related information or documents to external persons.
- Staff should not send emails to pupils.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

Mobile Phones and Devices

General use of personal devices

- Mobile phones and personally-owned devices should not be used in sight of pupils during school hours.
- No images or videos of children will be taken on mobile phones or personally owned devices.
- In the case of school productions, parents/carers are permitted to take pictures of their child only in accordance with school direction.
- With parental consent, pupils in Years 5 and 6 are allowed to bring a mobile phone to school to assist with independent travel to and from school. On arrival, pupils must ensure their phones are switched off and handed in to the main office for storing throughout the day. Pupils may collect their phone just prior to leaving the school.
- Pupils who do not follow the school policy relating to the use of mobile

phones will not be permitted to bring their mobile phones into school.

Pupils Publishing Content Online

- Pupils should only publish content onto school approved online learning platforms, as directed by class teachers.
- Pupils' full names will not be used on the school website, particularly in association with photographs and video.
- Permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must only be stored on the school network for such time as is necessary before deletion.
- Pupils and staff are not permitted to use portable devices to store images/video/sound clips of pupils.

Screening, Searching and Confiscation

The Department for Education's 'Searching, screening and confiscation, Advice for head teachers, school staff and governing bodies' (January 2018), allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity, exceptions will be made for staff working from home who may need to speak to a parent/carer as part of a parents meeting, with a pre-arranged time agreed. Staff must withhold their number.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- 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 devices will not be used during lessons unless permission has been granted by a member of the senior leadership team in emergency circumstances.

CCTV

- The school uses CCTV in some areas of school property as a security measure.
- Cameras are used in appropriate areas and there is clear signage indicating where it is in operation.

General Data Protection (GDPR) and Online Safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to online safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure:

- Care is taken to protect the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.
- Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.
- Any potential data breaches should be reported to the School Business Manager and/or the Head teacher within 72 hours, who may need to inform the Information Commissioner's Office (ICO).

Peer on Peer abuse and harassment

Connectivity between pupils and peers outside of school can give opportunity for abuse and harassment to occur. The school encourages parents to carefully monitor communication online and on mobile devices outside of school and advises that children are not left unattended with communication devices. Pupils are taught about their conduct online and in communication and are encouraged to be responsible citizens following the same behaviour principles and values we hold here at St Gabriel's.

Staff are aware that online abuse and harassment can violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online abuse and harassment, which might include non-consensual sharing of images and videos; sharing sexual images and videos (often referred to as 'sexting'); inappropriate upsetting or aggressive comments on social media; exploitation; coercion and threats.

Any reports of online abuse and harassment will be taken seriously, dealt with under the school's Behaviour and Preventing Bullying Policies. The school will involve parents when incidents occur and if necessary other agencies such as the police may be notified.

Appendices

Appendix 1

St Gabriel's C of E Academy

Pupil Acceptable Use Policy Agreement for KS1

Before using a digital device in school it is important you:

- Ask a teacher if you want to use a tablet or laptop.
- Only go on activities a teacher has given you permission for.
- Take care of the devices and other equipment.
- Ask for help from a teacher if you are not sure what to do.
- Let a teacher or teaching assistant know if you feel unsafe online or something upsets you.
- Do not share personal information like your passwords, address or photos online.
- Do not take photos of other children unless your teacher says you can.

To keep you safe online the adults in school may check what you have used a tablet or laptop for. You may not be given access to a device if you do not use it safely

Please sign below to show you understand and agree to the rules.

Class:

Signed:

Appendix 2

St Gabriel's C of E Academy

Pupil Acceptable Use Policy Agreement for KS2

Before using a digital device in school it is important you:

- Ask a teacher if you want to use a device.
- Understand the School will monitor your use to ensure you and others are safe.
- Keep your passwords safe and secure and do not share them with anyone.
- Sign out/ log off sites/apps which require a password.
- Tell your teacher if you think somebody else knows your password so they can change it
- Only use activities that a teacher has given permission to use.
- Take care of the devices and other equipment.
- Ask for help from a teacher if you are not sure what to do.
- Let an adult in school know if you feel unsafe online.
- Tell an adult in school if you see something that upsets you on the screen.
- Not to share personal information about yourself or others online.
- Understand you might not be given access to a device if you do not use it safely or appropriately.
- Do not take photos of others unless your teacher has given you permission.
- Know the School will help you if you are being bullied or upset on your devices at home.
- Understand you might have a consequence in school if you are disrespectful or rude to anybody in the school community (including children and adults) when online.
- Do not use personal devices such as mobile phones in school.

Please sign below to show you understand and agree to the rules.

Class:

Signed:

Appendix 3

ST GABRIEL'S CofE ACADEMY

Staff (and Volunteer) Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school can monitor my use of the school digital technology and communications systems.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the Academy Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the

email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a

suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name: .....

Signed: .....

Date: .....