E-Safety, Prevent Duty and Acceptable Use Policy

St Gerard's Catholic Primary School

"Guided by God, St Gerard's Catholic Primary and Nursery School is an inspiring and aspirational community where we learn to love, hope, dream and achieve."

Feb 2021

St. Gerard's Catholic Primary & Nursery School
E-SAFETY POLICY
Responsibilities

The member of school responsible for e-safety is Miss L. Roberts

They are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community. He/she may also be required to deliver workshops for parents.

Internet use and Acceptable Use Policies (AUPs)
All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. During Remote Learning this includes the Remote Learning Code of Conduct and the Risk Assessed Use of Zoom. (See Appendix 1- 6)

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip. (see Appendix 7)

The Remote Learning Code of Conduct will be sent to all parents/carers and available on the school website.

AUP's will be reviewed annually or as required. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Pupils must not take, use, share, publish or distribute images of others without permission
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Pupils' full names will not be used anywhere on a website or blog, particularly in

association with photographs.
• Permission from parents or carers will be obtained before photographs of pupils are published on the school website or twitter.
• Pupils' work can only be published with the permission of the pupil and parents or carers.

Photos and videos taken by parents/carers.
Parents and carers are not permitted to take photos/videos of their own children in school events. Parents attending school based events will be reminded of their responsibilities in relation GDPR May 2018.
The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)
Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices
St. Gerard's Catholic Primary & Nursery School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.
The concerns are mainly based around these issues:
- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones
St. Gerard's Catholic Primary & Nursery School allows staff to bring in mobile phones for their own personal use.
Staff:
- Staff must have their phones on 'silent' or switched off during class time.
- Staff may not make or receive calls during teaching time. If there are extreme circumstances (e.g. acutely sick relative) the member of staff will have made the Head Teacher aware of this and maybe allowed to have their phone on depending on the situation or reason. In this instance staff should not leave their classroom to use their mobile phone.
- Use of phones must be limited to non-contact time when no children are present.
- Phones must be kept out of sight (e.g. drawer, handbag, pocket) when staff are with children.
- Calls/ texts must be made/ received in private during non-contact time.
- Phones must not be used in classrooms.
- Phones will never be used to take photographs of children or to store their personal data.
- The use of Mobile Phones is prohibited whilst in control of a car. All staff are aware of this.

Emergencies
Staff are instructed that they can use their mobile phones in the event of an emergency situation' i.e. lockdown situation.

If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. Staff must ensure that there is no inappropriate or illegal content on the device. Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the nursery/school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.
Members of staff may only contact a parent/carer on school approved mobile phones.

Pupils:
- Pupils are not permitted to use mobile phones, they may bring them to school and leave them with the Office Staff in order for parent/carers to contact them before and after school if the children are walking to school/home by themselves.
- The parent must inform the Headteacher and the class teacher.

- The phone must be handed in, switched off, and handed to the school office in the morning and collected by the child at home time (the phone is left at the owner's own risk).

Where a pupil is found to be using a mobile phone at school, the phone will be confiscated from the pupil and handed to a member of the office team who will record the name of the pupil and attach it to the phone to store it until the end of the day. Should a pupil be found to be using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the main or the manager's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

Signs are visible within the school grounds informing any visitors to school cannot use their mobile phones.

Parents/carers:
While we would prefer parents not to use their mobile phones at school, we recognise that this would be impossible to regulate and that many parents/carers see their phones as an essential means of communication at all times. We therefore ask that parents' usage of mobile phone, whilst on the school site is courteous and appropriate to the school environment. If parents and carers use their mobile phones to take pictures during assemblies we act that they do not post them to social networking sites.
We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and
inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails
Pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords
Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').
All users should be aware that the ICT system is filtered and monitored.

Data storage
Only encrypted USB pens are to be used in school.

Reporting
All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.
Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.
Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to Mr J. Greenwood in the same day.
Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.
Evidence of incidents must be preserved and retained.
The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

Remote Learning

Please read in conjunction with Remote Learning Policy Feb 2021 & Addendum to Safeguarding Policy January 2021

St Gerard's will continue to provide a safe environment, including online. This includes the use of an online filtering system.

Where students are using computers in school, appropriate supervision will be in place. Please see the schools Remote Learning Policy for more detail on this area.

Children and online safety away from school
It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care (iCART) and as required, the police.
Online teaching should follow the same principles as set out in the staff code of conduct.

St Gerard's will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
Below are some things to consider during lessons, especially where webcams are involved:

•No 1:1s, groups only
•Staff and children must wear suitable clothing, as should anyone else in the household.
•Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred, if possible.
•The live class should be recorded so that if any issues were to arise, the video can be reviewed.
•Live classes should be kept to a reasonable length of time, to avoid excessive periods of screen time.
•Language must be professional and appropriate, including any family members in the background.
•Staff must only use platforms specified by senior managers and approved by the school's IT network manager / provider to communicate with pupils
•Staff should record, the length, time, date and attendance of any sessions held.

(Please refer to Parent Code of Conduct and the Remote Learning Code of Conduct for Further information)

We will 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 learning platform – Dojo, Seesaw and use of Zoom for whole class sessions. We will also provide technology where possible. Paper based packs will be available for all parents that would prefer this.
(Please see the Remote Learning Policy for the plan and detail)
We expect pupils to follow the same principles, as outlined in the school's Acceptable User policy whilst learning at home. This is further detailed in the Remote Learning Code of Conduct and the Risk assessment produced for the use of Zoom and for technology provided to families on request.
If St.Gerard's Primary and Nursery School chooses to communicate with pupils via Microsoft Teams or Zoom then it is important that this is only carried out with the approval of the Head teacher or the remote Learning Lead – the Deputy Head teacher.
Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting. The chat function within Microsoft Teams is to be disabled to avoid distractions from learning and potential cyber-bullying.
If providing a video for pupils teachers will be asked to sit against a neutral background, avoid recording in bedrooms, dress appropriately, check tabs open in the browser are appropriate if sharing screens and use professional language. Pupils will also be expected to be in a shared space in their house and dressed appropriately (alternatively have their cameras switched off). Parents who are present will also be expected to be mindful that other children might see or hear them. A recording of the video is to be made for school records only.
Any significant behavioural issues occurring on any virtual platforms must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

Infringements and sanctions
Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the SLT in line with the Behaviour Policy.
The following are provided as exemplification only:
Level 1 infringements:-
- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone or use of lapdop/ IPad]

Level 2 infringements:-
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Unauthorised use of mobile phone (or other new technologies)
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing software
- 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

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements:-
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately 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.
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer] Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

School is 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.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – e.g. Dojo points, Headteacher award, Computing Weekly Award, Good to be Green awards.

Social networking

Pupils are not permitted to use social networking sites within school.

E-Safety Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

- A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- Regularly auditing, review and revision of the computing curriculum
- E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
- Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc.

Additionally,

- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour

Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

- A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
- E-safety training is an integral part of Child Protection / Safeguarding training and vice versa

- All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
- Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
- The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
- The school takes every opportunity to research and understand good practice that is taking place in other schools
- Governors are offered the opportunity to undertake training.

Parents and the wider community

There is a planned programme of e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinator with input from the e-safety committee.

Monitoring and reporting

- The school network provides a level of filtering and monitoring that supports safeguarding.
- The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Halton Local Authority (where necessary)
- Halton Safeguarding Children Board
- The school action plan indicates any planned action based on the above.

Online safety away from school

Online teaching should follow the same principles as set out in the staff code of conduct.
St Gerard's will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
While delivering online learning, you must consider these things, especially where webcams are involved:

- No 1:1s. Lessons with groups online
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred, if possible.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept at a reasonable length of time, to avoid excessive periods of screen time.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by the school's IT network manager / provider to communicate with pupils.
- Staff should record, the length, time date and attendance of any sessions held.

Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters.
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device lock if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing antivirus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.

Rules for children to adhere to while working remotely:

- I will only use technology for school purposes as directed by my teacher.
- I will only use technology when there is an adult in the house and they know I am using it.
- I will not reveal my passwords to anyone.
- I will be responsible for my behaviour and actions when using technology (Zoom, SeeSaw, ClassDojo and other applications), this included the resources I access and the language I use.
- I will make sure that all my communication with pupils, teachers and others using technology is responsible and sensible.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidently come across such material, I will report it immediately to my teacher or my parents.
- I will not record or take photos of my classmates or teachers during any remote learning sessions.
- I understand that when using ClassDojo and other application agreed by the school that my use is monitored and logged and can be made available to my teachers.

Safeguarding

Please refer to the schools Safeguarding policy and the appendum regarding school closure and Covid-19 for further information on safety while working remotely.

St. Gerard's Catholic Primary and Nursery School

Appendix 1

Acceptable Use Policy for learners in KS1

I want to feel safe all the time.

I agree that I will:

- **always keep my passwords a secret**
- **only open pages which my teacher has said are OK**
- **only work with people I know in real life**
- **tell my teacher if anything makes me feel scared or uncomfortable on the internet**
- **make sure all messages I send are polite**
- **show my teacher if I get a nasty message**
- **not reply to any nasty message or anything which makes me feel uncomfortable**
- **not give my mobile phone number to anyone who is not a friend in real life**
- **only email people I know or if my teacher agrees**
- **only use my school email**
- **talk to my teacher before using anything on the internet**
- **not tell people about myself online (I will not tell them my name, anything about**
- **my home and family and pets)**
- **not upload photographs of myself without asking a teacher**
- **never agree to meet a stranger**

Anything I do on the computer may be seen by someone else.
I am aware of the CEOP report button and know when to use it.

Child's Name ……

Class ……

Date……

St. Gerard's Catholic Primary and Nursery School

Appendix 2

Acceptable Use Policy for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

1. I am aware of the CEOP report button and know when to use it.
2. I know that anything I share online may be monitored.
3. I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Child's Name ……

Class ……

Date……

Appendix 3 - Acceptable Use Policy for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

- I agree that I will not:
  visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.
- I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.
- I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____ Your name (in block capitals): .....

Date:.....

St. Gerard's Catholic Primary and Nursery School

Appendix 4

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Signed _____

Your name (in block capitals): .....

Date:.....

Appendix 5 - Remote Learning Code of Conduct

St Gerard's Catholic Primary School

"Guided by God, St Gerard's Catholic Primary and Nursery School is an inspiring and aspirational community where we learn to love, hope, dream and achieve."

Online Remote Learning Responsible User Agreement

Remote Learning Code of Conduct

This code of conduct outlines what we expect of children and parents/carers during remote learning. Much of this echoes our expectations of children in lessons when in school and all of it is designed to help children gain the most benefit from online learning. Parents/Carers must read the following information and then by logging on to any of the school's platforms for learning, this confirms they agree to this code of conduct. St Gerard's will not be held responsible for any incidents that occur if the code of conduct has not been followed.

- Myself and my parents/carers, will check my Dojo and Seesaw at least daily to keep track of online sessions and learning.
- I will only use technology provided by school for school purposes as directed by my teacher.
- I will not reveal my passwords to anyone other than my parent/carer.
- Myself and my parents/carer understand that my teacher will only be available to give live feedback or take calls between 9:00am and 3:00pm.
- I will only use Seesaw, Dojo and Teams as directed by the teaching staff and will only upload material that is related to my learning.
- I will not take photos of my screen or record videos or interactions in any way (on all digital platforms – Dojo, Parent App, Seesaw, Teams or Twitter) other than to upload my own work.
- I will make sure that my communication in the online learning environment (Dojo, Seesaw, TT Rockstars, Twitter, Email and Teams) is always supportive of my learning and the learning and wellbeing of others.
- I will be responsible for my behaviour and actions when using Dojo, Seesaw, Twitter or Microsoft Teams, this includes the resources I access and the language I use.
- I understand that my parent/carer is responsible for logging into Teams and the meeting details if required.
- During any live sessions, my parent/carer must be present in the room or in the next room with the door open so they can see and hear everything that is happening during the live session.
- If taking part in a live sessions I will make sure that...
  - my environment is quiet and free from distractions
  - the background (and foreground) is appropriate and as neutral as possible (please be mindful of what is visible behind you/in front of you)
  - I am appropriately dressed
  - I remain attentive

- Any live sessions will be recorded by the class teacher for safeguarding purposes.
- When accessing live sessions -just like in class, I will use the 'hands up' button when I want to speak and will try not to talk over anyone else – the teacher will be able to mute me as required.
- The teacher reserves the right to remove you from any digital learning if they see/hear anything that does not follow the Remote Learning Code of Conduct.
- I will make sure that all my communication with peers, teachers or others using technology is responsible and sensible. I will be respectful as I would within the classroom.
- I will not deliberately browse, download, upload or forward material that I should not be viewing. If I accidentally come across any such material, I will report it immediately to my teacher or my parent/ carer.
- I will not share resources or videos created by my teachers with anyone who is not a pupil or member of staff at St. Gerard's Primary School.
- I will not record or take photos of my classmates or teachers
- I will not share any school content on social media platforms.
- I will not share personal details about myself, my family or others I know on any platforms.
- I understand that when using the online platforms provided by the school that my use can be monitored and logged and can be made available to my teachers.
- If audio/video conferencing is used, I understand that this will be recorded by the teacher only to share with pupils to be able to continue to learn outside of the time of the lesson itself.
- I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parents will be contacted.

By logging your child on to the learning platform or live session, you are agreeing to the Remote Learning Code of Conduct and the rules and guidelines set out by your child's class teacher.

Remember when using any form of social media, whatever you type or upload, is always there and you can't take it back. So be mindful of what you say and write.

All material recorded by school staff, is the property of St. Gerard's Primary School and is not to be shared, downloaded or saved by anyone other than a member of St. Gerard's Primary School staff. You MUST NOT record each other online. When the **live meeting is recorded, this can only be done by the teacher.** (Make sure you end the live session as soon as the teacher indicates to do so and do not stay in the session after the teacher has left.)

General Guidelines

-It is recommended that you follow the school timetable each day as far as possible.
-Please complete tasks as they are set for each lesson. Teachers will be available at the times when they would normally be teaching you in order to answer questions and give feedback via the school's online platform.
-If possible, upload any work onto Seesaw or Dojo as soon as you complete it so your teacher can provide feedback.

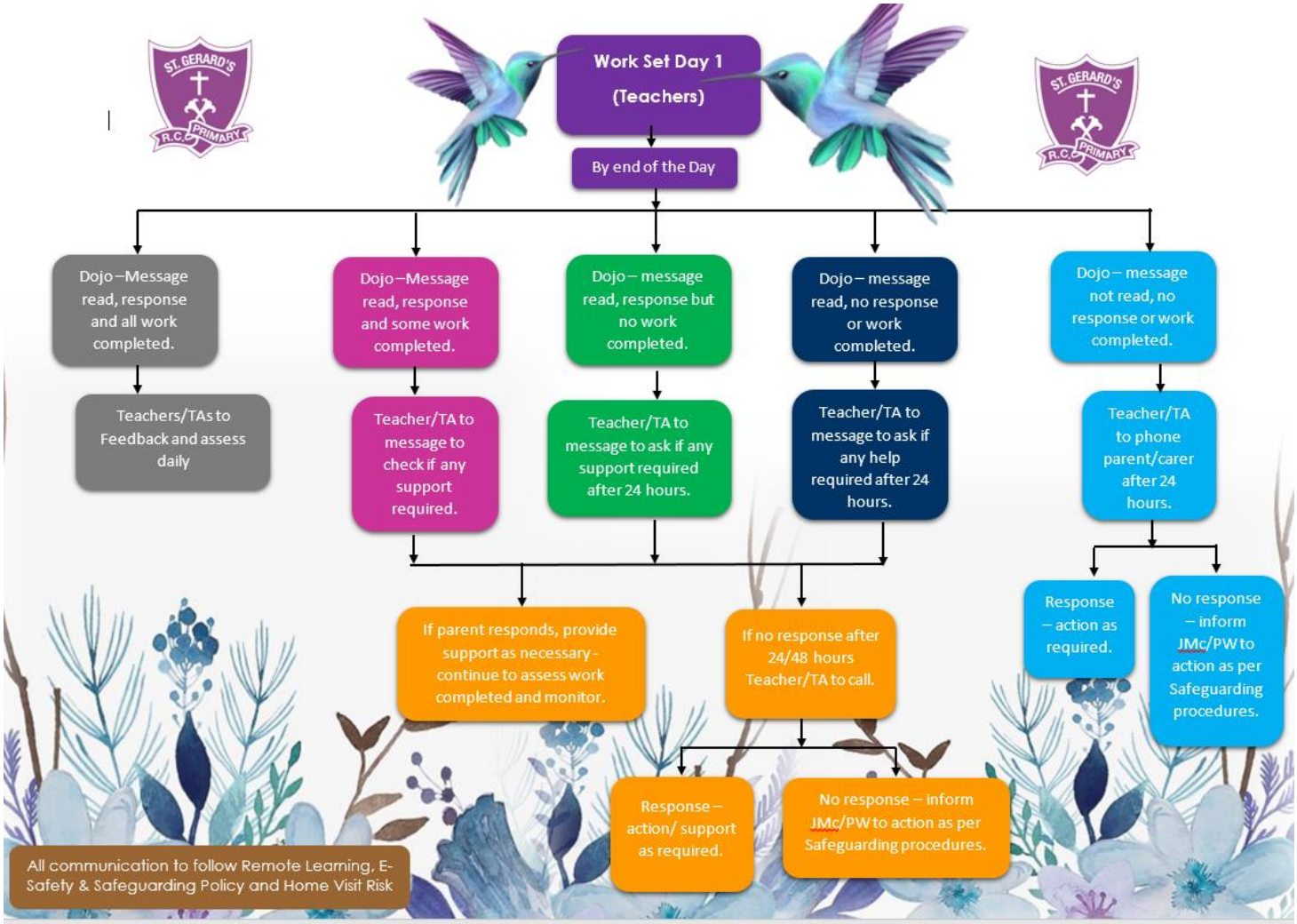
Parental Support

-Ensure an adult is available to support with any technical issues.
-Check parental controls on the device.
- Discuss e-safety principles with your child – there are various links to information and advice on the Remote learning page of the school website
- Report any concerns to school immediately.
-Please encourage children to access remote learning at the correct times.
-Please encourage children to show respect through their comments and behaviour when learning remotely.
-To be aware that **live meetings may be recorded by the teacher.**
-To be aware that **only the teacher is allowed to share recorded live activities or lessons**.
-If you need to contact the teacher about something urgent then please use the class Dojo or Seesaw or contact the school office.

Please see the flow chart of "Securing Engagement of Remote Learning".

Schools have a duty to check daily whether pupils are engaging with their work, and work with families to rapidly identify effective solutions where engagement is a concern.
Schools also have a duty to ensure that all children are safe. The engagement of your child with the remote learning provision is part of our statutory safeguarding responsibilities.
The Keeping Children Safe in Education (2020) document, updated January 2021, clearly indicates that teachers are well placed in their professional capacity to identify those children whose behaviour suggests they may be at increased risk of experiencing mental health issues.
In prioritising our safeguarding responsibilities and supporting parents and carers we need implement the following protocol to keep all children safe from mental health issues when learning remotely online.

A. Where a child is meaningfully engaging in the learning in a timely manner and as expected then no further action is required.
B. Where a child is not meaningfully engaging in the learning as expected then the following steps will be actioned.



Appendix 6

Risk Assessment – Use of Zoom Online Platform

Date completed: 04/02/21	**Assessed by: Jane Gilbert** **Authorised by : Karl Landrum**
Review date: as and when required	Identification of those at risk: Pupils School staff Parents/Carers

Possible risks/hazards	Measures put in place	Who is responsible for measures?	What is the risk now?
Lack of supervision by parents/carers	Parents/carers asked to make themselves known to the host and asked to stay close to the child for the meeting Parents/carers asked to log in for the child with information provided by the class teacher https://www.saferinternet.org.uk/blog/what-%E2%80%A6-zoom-guide-parents-and-carers#How%20Zoom%20works	Staff setting up meeting	Low
Members of the public attending – no invited guests	Waiting room set up by staff – staff to verify the child is the child they are expecting	Staff setting up meetings	Low
Area used in chat by staff member and child	Staff and parents/carers to ensure that background area is free from personal items. https://support.zoom.us/hc/en-us/articles/210707503-Virtual-Background Address issues with any child's background if needed Staff have pre-recorded videos	Staff setting up meetings	Low
Children to not be in room being used alone	staff to set up zoom meeting username and passwords Check once sessions starts that an adult is present in the room	Staff setting up meetings	Low
Adult or other children acting inappropriately by accident or deliberately	A second member of staff will be present Staff can mute/unmute and remove if necessary Staff can control cameras	Staff setting up meetings	Low
Parents passing on Zoom Meeting Details to others	Parents/carers told that they must not give meeting details to others. They must direct other parents to school staff to gain information.	Staff to inform parents. Parents/carers to follow advice.	Low

Appendix 7

St. Gerard's Catholic Primary and Nursery School

Lugsdale Road, Widnes, Cheshire, WA8 6DD
Tel: 0151 424 2879 Fax: 0151 424 4461

Headteacher – Mr K. Landrum – BEd (Hons) NPQH

Website: http://st-gerards.halton.sch.uk

Parent/Carer name:……..

Pupil name: …….. class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' signature:……

Your name (in block capitals): ……

Date:…… …….

St. Gerard's Catholic Primary and Nursery School

Appendix 8

School audit
Audit
The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Halton guidance?	Yes
Date of latest update (at least annual):	Autumn 2020
The Leadership team member responsible for e-safety is:	Mr Landrum
The governor responsible for e-Safety is:	Mrs C Godwin
The designated member of staff for child protection is:	Mr K. Landrum
The e-Safety Coordinator is:	Miss L. Roberts
The e-Safety Policy was approved by the Governors on	
The policy is available for staff at:	School website and policy file
The policy is available for parents/carers at:	School website
Date of E-safety training for staff	March 2021
Date of Prevent training	September 2020

Appendix 9

Photo/video consent
School Name:
Name of pupil:
Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.
To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please bring the completed form to the ceremony. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

May we use your child's image in our printed promotional publications?	Yes / No
May we use your child's image on the school website/SLG?	Yes / No
May we record your child's image on our promotional videos?	Yes / No
May we use your child's image in the local press?	Yes / No

Signature: ……..

Your name (in block capitals)…….

Date: ……: