Giffards Primary School

Online Safety Policy

(including acceptable use agreement policy)

School lead for this policy:	Mrs N Haslam-Davis
Committee with oversight for this policy	FGB
Policy last reviewed	December, 2021
Date for next review	Annually December 2022
Signed –chair of Governors	
Signed - Headteacher	Mrs N Haslam-Davis

Development/Monitoring/Review of this Policy

Introduction

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/academies are bound. Schools/academies must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school when using school devices. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.
In England, schools/academies are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. From 2015, additional duties under the Counter Terrorism and Securities Act 2015 require schools/academies to ensure that children are safe from terrorist and extremist material on the internet. Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place.
Due to the ever changing nature of digital technologies, we will follow best practice and review the Online Safety Policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

This online safety policy has been developed by a group made up of:

- Headteacher and senior leaders
- Online Safety lead
- Staff – including teachers, support staff, technical staff
- Governors

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*July 8th 2021*
The implementation of this online safety policy will be monitored by the:	*Online Safety lead–Miss Hammerton Leadership Team (HT and SLT)*
Monitoring will take place at regular intervals:	*annually*
The Governing body will receive a report on the implementation of the online safety policy generated by the Link2ICT monitoring reports (which will include anonymous details of online safety incidents) as part of the safeguarding report to Governors:	*Termly reports of online safety incidents Annual review of policy implementation*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually from approval*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents – 1 x termly report of inappropriate use from staff/pupils as part of safeguarding report to FGB
- Monthly Monitoring logs of internet activity (including sites visited)/filtering / and immediate - serious concerns

Related policies

- Social Networking Policy
- Code of Conduct + LLC policies
- Password Protection policy
- Mobile Phone and Personal Devices/Technologies Policy

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the schools site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, Mr D Stubbings has taken on the role of Online Safety Governor as part of his role as the Child Protection Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety lead
- regular monitoring of online safety incident logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Lead.*
- The Headteacher and Mrs V Teager (DSL) will respond to all reported incidents of online inappropriate use by pupils/staff. See flow chart **appendix B** on dealing with online safety incidents – "Responding to incidents of misuse" and relevant disciplinary procedures.
- The HT and Business Manager receive regular monitoring reports from our monitoring provider Link2ICT

Online Safety Lead

Miss S Hammerton (and Mrs V Teager)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- provides training and advice for staff
- liaises with school technical staff
- receives reports of pupil online safety incidents (kept by Mrs S Bryant as generated from Link2ICT Digital Monitoring Service who creates a log of incidents to inform future online safety developments)

Network Manager/Technical staff

Technical staff – **Mrs S Bryant** (Business Manager) **Mr A Hedges** (0.5 days a fortnight)

IT Technician – tbc (Part Time)

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required online safety technical requirements and any other guidance that may apply.
- that users may only access the networks and devices through a properly enforced password policy . See policy + **see Technical Security appendix E**
- the filtering by Thurrock Broadband is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored (by Link2ICT Digital Monitoring Service) in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of this school online safety policy and practices – they must ensure online safety issues are embedded in all aspects of the curriculum and through computing and PSHE (see coverage in computing and PSHE schemes of work). It is signed for on appointment to the school and if there are subsequent amendments. Other relevant policies that must be read are above including the Mobile Phone and personal devices/ technologies Policy and social networking policy.
- they have read, understood and signed the staff acceptable use policy agreement (AUPA) **appendix D**
- they report any suspected misuse or problem to the Headteacher//Senior Leader/Online Safety Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- activities
- pupils understanding and following the Online Safety Policy and acceptable use policies – **appendix A**
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- If staff have any concerns about a child's welfare, they must act on them immediately and speak with the designated safeguarding lead (or deputy) – they must not assume that others have taken action.

Designated Safeguarding Lead/Designated Person/Officer

Mrs V Teager

Is trained in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of Mobile Phone and personal devices/ technologies Policy. They should also know and understand the school policy on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school and/or using a school device.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school/academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events **appendix A**
- access to parents' sections of the website
- their children's personal devices in the school

Community Users (e.g. student teachers/visitors who require IT access)

We do not allow access to the school wifi to any external devices/visitors , this is due to the way the filtering system works. All school based devices run our monitoring software and we are unable to allow access to devices without this. Additionally our system requires an additional security certificate to be installed to enable access to the internet.
For school based community users, such as SCITT students, we provide devices which may be used with a school based log. Users who access school systems or programmes as part of this provision will be expected to sign a Community User AUA before being provided with access to a school device/systems.

Policy Statements

Education – Students/Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and should he regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies and PSHE activities
- 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.
- Students/pupils should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. All school owned devices are monitored.

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents workshops
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school/academy will provide opportunities for local community groups/members of the community to gain from the school's/academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school/academy website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to staff and individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school/academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).
- Online CPD through our school provider

Teaching pupils about Online safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group [ ]

We also focus on developing a fifth C – **confidence**. Woven through our broad, balanced curriculum, our core values, PSHE lessons and assemblies we teach pupils how to identify unsafe behaviours, such as peer to peer abuse*, including online abuse and bullying, and how to build the strength and resilience to deal with these and who to turn to for help.

***Peer to peer abuse which may be linked to online safety**

Peer on peer abuse is most likely to include, but may not be limited to:

• *bullying (including cyberbullying, prejudice-based and discriminatory bullying);*

• *abuse in intimate personal relationships between peers;*

• *physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse);*

• *sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence);*

• *sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse;*

• *causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party;*

• *consensual and non-consensual sharing of nudes and semi nudes images and or videos (also known as sexting or youth produced sexual imagery);*

• *upskirting, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; and*

• *initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).*

Online safety -Child safety policy

The school's approach to dealing with, recording and reporting, Online safety including digital devices is detailed in our child protection policy. The protocols to follow are detailed in this policy

Remote learning

As part of our online safety support for pupils, pupils use a school owned chrome book when self-isolating, these are monitored remotely and any safeguarding concerns reported to us and followed up. all chrome books are named and have attached to the cover a copy of the child's signed AUA and protocol for safe use (as agreed by the children through school council)

see KS1 and KS2 acceptable use agreements below and

Appendix F - Chromebook - Home Loan Agreement

Appendix G - Remote teaching using technology and on-line devices

Monitoring on-line safety

Our monitoring system reports captures of any inappropriate use of school owned systems.

Staff must be vigilant to indicators and signs of online abuse including Peer on peer abuse. Peer on peer abuse can manifest itself in many ways. This may include bullying, including cyber bullying – see above*. We do not tolerate any harmful behaviour in school and will take swift action to intervene where this occurs. We use lessons and assemblies to help children understand, in an age-appropriate way, what abuse is and we encourage them to tell a trusted adult if someone is behaving in a way, including online or via digital devices, that makes them feel uncomfortable.

Raising Concerns

If staff have any concerns about a child's welfare, they must act on them immediately and speak with the designated safeguarding lead (or deputy) – they must not assume that others have taken action. All staff members are aware of and follow school processes (as set out in the Child protection policy) and are aware of how to make a referral to Social Care if there is a need to do so.

See below - Reporting incidents- recorded and reported by V Teager – DSL, this details how staff should respond to incidents of misue

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username to log onto the school system. For online programmes pupils are provided with a user name and password. Subject leaders are responsible for by keeping an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- The Business Manager – Mrs S Bryant, is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Thurrock broadband and monitored by Link2ICT. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering between staff and pupils

- Link2ICT monitor and record the activity of users on the school technical systems and report any inappropriate behaviour/actions to the school HT and Business Manager. Users are made aware of this in the acceptable use agreement and there is a reminder every time a device is booted up that has to be agreed to.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person - referring to the Business Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual devices are protected by up to date virus software.
- No downloading executable files and/or installing programmes on school devices is allowed unless by prior permission.
- Only encrypted memory sticks/external devices are allowed but never for the transfer of personal or school data. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should is inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy and acceptable use policy.
Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give cousideration to the use of mobile technologies

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Who does this apply to	**• Staff employed by the school who have or use a laptop/PC/ chromebook for school use and off site usage • Students on placement– have access to school owned devices**	**Staff using ICT suite/class based computers**	**Staff using school owned ipads /cameras/ chromebooks**	**Only mobile phones are allowed**	**All staff**	**All visitors**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes* In line with Mobile Phone and personal devices/ technologies Policy – older pupils may bring a phone at own risk. These must be on silent and kept in a bag. Usage on premises is strictly forbidden	*Yes* On silent and only accessed during breaks/ after directed hours unless permission has been given – Mobile Phone and personal devices/ technologies Policy	*Yes* See mobile phone policy
Full	*Yes*	*Yes*	No access	*NO*	*No*	*NO*

network access			to school server			
Internet only	The school has 2 laptops for use by students on placement – these have full proxy and server access and are monitored	*yesd*	*yes*	*No* No devices bought to school, including mobile phones should have access to school internet	*No* No staff devices bought to school, including mobile phones should have access to school internet	Visitors may with the permission of the head and upon installation of relevant security certificate access the wireless network – **see permission slip for AUA**
No network access				No network access	No network access	No network access unless by prior permission from HT/Business Manager - **see permission slip for AUA**

School owned/provided devices:

All school owned devices must be added to the devices register kept by the IT technician

- **Who they will be allocated to:**

  The school will allocate laptops to all teachers. Laptops may be made available for other staff depending on their job role. Other devices such as cameras/ipads are available for classroom use and will not be added to the school network. The location of these are logged by the IT technician
  Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately. Costs to damage of IT equipment off site should be claimed through staff members own contents insurance.

- **Where, when and how their use is allowed – times/places/in school/out of school**:

  All school owned devices such as computers and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy (and the Acceptable Use Agreement and Code of Conduct).
  Classroom computers must not be moved from the class base.
  Laptops may be used in school and can be taken of site by staff with permission.
  Chrome books are primarily for use in school, permission must be given (and recorded) if devices are taken off site/used at home.

  Other devices such as cameras are for use in school/school trips but must not be taken home unless permission has been given.
  Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

  Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is

- 1. Discriminatory or harassing;

- 2. Derogatory to any individual or group;
- 3. Obscene, sexually explicit or pornographic;
- 4. Defamatory or threatening;
- 5. In violation of any license governing the use of software; or
- 6. Engaged in for any purpose that is illegal or contrary to the school policy or interests.

Personal use

School equipment, internet services, systems and email may be used for staff incidental personal purposes, with the approval of the line manager, provided that it:

• does not interfere with the school's operation of computing facilities or email services;

• does not interfere with the user's employment or performance of professional duties or other obligations to the school;

• is of a reasonable duration and frequency;

• is carried out in authorised break times or outside their normal working hours;

• does not over burden the system or create any additional expense to the school;

• is not uses to access, send, receive or store inappropriate material; and

• does not bring the school and its community into disrepute.

- Workers must notify the school of any significant personal use.
  Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.
  Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

  School equipment/networks/systems must additionally not be used for

  • commercial purposes not under the auspices of the school;

  • personal financial gain;

  • personal use that is inconsistent of other school policies or guidelines; or
- School equipment should not be used by any other family member/anyone else

Levels of access to networks/internet (as above)

Staff in receipt of a school laptop/computer (excluding ipads/chrome books) will have access to the staff on server drive of the curriculum server. The Business Manager has full access to both Curriculum and Admin server in school as well as remotely.

Users must not:

- use, transfer or tamper with other people's accounts and files; this includes deleting school files and information even if created by the staff member.
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;

- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

Loaning devices to pupils for use at home

Chromebooks may be loaned to pupils, upon completion of a loan agreement – **see appendix F** for the benefit of the child in supporting and developing their education, this is primarily for use during enforced closure/quarantine when remote learning expectations are in place.

- The loan agreement exists between the school and the parent/carer who must signed the loan agreement. This is to include

    - Pupil Name:
    - Parent/Carer's Name & Address:
    - Chromebook Serial Number

- the chromebook will be loaned to the parent/carer for the duration of the period in which the child within their care needs to access IT for remote learning
- When the child no longer needs to work from home/self-isolate they will need to return the chromebook by an agreed date.
- Should the family/child move address from the address given, parents must inform the school at the earliest opportunity.
- Parents will be issued with a chromebook and power supply. These remain the property of Giffards Primary School.
- The Licensed software for use is already installed on the chromebook. At no point must the chromebook be opened or changes made to the inner hardware or any other software be downloaded. No personal documentation or work should be stored on the chromebook.
- The chromebook and the connectivity equipment must not be used for any illegal and/or antisocial purpose. Included within the chromebook is software that monitors all keystrokes and the school will be alerted to any inappropriate use. This is part of our safeguarding obligations.
- There may be occasions when we need you to return the chromebook to school for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the chromebook. Giffards Primary School cannot be held responsible for the loss or damage of any data on the chromebook during this process. It is your responsibility to return the chromebook to school.
- All technical support and maintenance must go through Giffards Primary School, please contact us if your child experiences any issues.
- If your chromebook is stolen you must immediately report it to the police and get a crime reference number. Then immediately report this to us; we will make every effort to replace the chromebook when we are able.
- If the chromebook is damaged/broken parents will be liable for any repair costs, if the chromebook is damaged beyond repair or lost parents are liable for replacement costs (new for old). We will do our best to repair the damage, if this is not possible, replacement will be on a case by case basis.

Responsibilities you have to care for your chromebook:

- Parents/child have a responsibility to take reasonable care to ensure the security of the chromebook and connectivity equipment.

- The chromebook provided must not decorated or the external face change of the equipment changed in any way in any way, including affixing stickers.
- Reasonable health and safety precautions should be taken when using a chromebook. The school is not responsible for any damage to person or property resulting from the chromebook or equipment loaned.
- The school is not responsible for any costs resulting from the use of the chromebook and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.
- Breach of the above conditions may result in the loan of the chromebook being withdrawn by the school.

- **Management of devices/installation of apps/changing of settings/monitoring**

  All school owned devices have a monitoring system and staff must not tamper with or remove this. All school equipment is monitored even when working remotely/from home
  Staff must sign to agree to this monitoring each time the device is used.

  To prevent computer viruses from being transmitted through the school's computer system, unauthorised downloading of any software is strictly prohibited. Only software registered through the school may be downloaded. Employees should use virus trapping software on any home computer that is used to download planning or other information onto the school computers. Employees should contact the head teacher/Business Manager if they have any questions.

Technical support

Technical Support is available from the IT technician, and in their absence the Business Manager, staff are expected to send an email with their technical request if there is an issue.
Curriculum support is available from S Hammerton – IT lead

- **Data Protection**

  The school follows sound professional practices to secure data, system programmes, email records and networks under its control.
  Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:
  • using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;

  • ensuring all devices and system access are password protected Using secured memory sticks (all laptops, memory sticks and devices used must be encrypted);

  • ensuring that pupils are not exposed to any inappropriate images or web links; and

  • respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Exit processes – what happens to devices/software/apps/stored data if user leaves the school

- All school owned devices must be returned to the school Business Manager before a member of staff leaves.
- No information should be deleted from the school network system or school used cloud based services
- Personal devices - the Employee shall, before their exit date, erase irretrievably any information relating to the business or affairs of Giffards Primary(or its business contacts) from computer and communications systems and devices owned or used by them outside the premises of the school, including such systems and data storage services provided by third parties (to the extent technically practicable).
- All passwords will be changed and access to school systems will be terminated

Personal devices: see Mobile Phone and Personal Devices/Technologies policy

- No mobile devices whether owned by staff, pupils or visitors may be connected to the school internet and must not have network access – see Mobile Technologies (including BYOD/BYOT) section above
- Usage for staff is restricted to break/lunch times or after directed hours unless prior permission has been given. These are detailed in the Mobile Phone and Personal Devices/Technologies Policy
- Pupils are forbidden to use any phone/mobile device on school premises
- Mobile Phones for work related purposes are allowed in accordance with our Mobile Phone and Personal Devices/Technologies policy
- The school has the right to take, examine and search users devices in the case of suspicion of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- No personal device should be used for taking/storage/use of images unless prior permission has been given by the headteacher
- All personal mobile phones and devices are bought in to the school at the owners risk. The school cannot accept liability for loss or breakages
- Visitors to the school should have their phones on silent or switched off and out of sight of children, this will be explained by admin upon entering the school
- Mobile phones should not be used in a space where children are present

Mobile Phones - *see also use of Mobile Phone and Personal Devices/Technologies Policy*

It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time. Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks.

Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile outside of breaks must get permission from the Headteacher.

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must he kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

No pictures or videos may be taken within school or at any school related activity, on personal devises.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press - these are saved in the admin office and MIS
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving staff or other pupils in the digital/video images.

Use of images – guidance to be followed

School/academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with this policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student/pupil pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Students/pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images.
- Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes unless in exceptional circumstances and prior permission by the headteacher has been given.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' names will not be used anywhere on a website or blog, particularly in association with photograph. There should be nothing to identify where the child lives.
- Images sent to staff, such as when participating in events/competitions must follow the guidance here even if parents give permission for more details to be included .
- No photos or video are to be taken on personal mobile phones (unless by prior permission from the Headteacher – see Mobile Phone and personal devices/ technologies Policy) when on school property or school business such as trips/visits/sporting events. Only school cameras/Ipads must be used and all content downloaded to a school computer.
- All photos/images taken in school will be stored on the school network server and deleted in accordance with GDPR

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- holds only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents and volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held ahout them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- understands how to share data lawfully and safely with other relevant data controllers.
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.

- device must be password protected.
- device must be protected by up to date virus and malware checking software

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

When using communication technologies, the school/academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and can be monitored. Users should be aware that email communications can be monitored. Staff and students/pupils should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Business Manager –the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with google classroom and other programme log ins and maybe provided with individual school email addresses for educational use.
- Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not he posted on the school/academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity – see also Social Network policy

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there is:

- A process for approval by senior leaders/headteacher
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
  any abuse and misuse must be reported to the Headteacher/School Business Manager
  Incidents that are in breach of this and other associated policies may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites outside of school hours

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school does not routinely respond to school social media comments, where comments are made they should be in line with this policy.

The school's/academy's use of social media for professional purposes will be checked regularly by the SLT to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepnte				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Any such misuse will be dealt with under the schools HR disciplinary policy and may be referred to the police. Serious or repeat offences will automatically be reported to the police.						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of tbe internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming N.B - (educational) for school based educational games where downloads have been authorised such as TTRS			X			
On-line gaming (non-educational)					X	
On-line gambling					X	

On-line shopping/commerce N.B. - out of working hours only		X			
File sharing (e.g. Loom/youtube/google classroom) any clud based files must follow GDPR guidance and be approved	X				
Use of social media N.B. – *1 out of working hours only *2 staff nominated as school social media users		X*1	X*2		
Use of messaging apps -			X		
Use of video broadcasting e.g. Youtube (staff must check appropriateness) any uploading of clips to youtube must be authorised by the Headteacher/SLT and be uploaded by a nominated member of staff	X				

Reporting incidents- recorded and reported by V Teager - DSL

Our monitoring system reports captures of any inappropriate use

Each capture is graded a level of severity on a scale of 1 - 5. If any captures showing grade 3,4 or 5 are detected, Link2ICT will flag this with school with an explanation as to why, the school will then investigate and a response from school is always required. Mrs Haslam-Davis (headteacher), Mrs Teager(DSL) and Mrs Bryant (Business Manager) are alerted by email to any Grade 3, 4 and Grade 5 captures requiring attention. These are logged to our online Safeguard system as Captures and actions that are taken are logged. All our actions and comments are recorded. Captures are graded in accordance with the following Risk Levels:

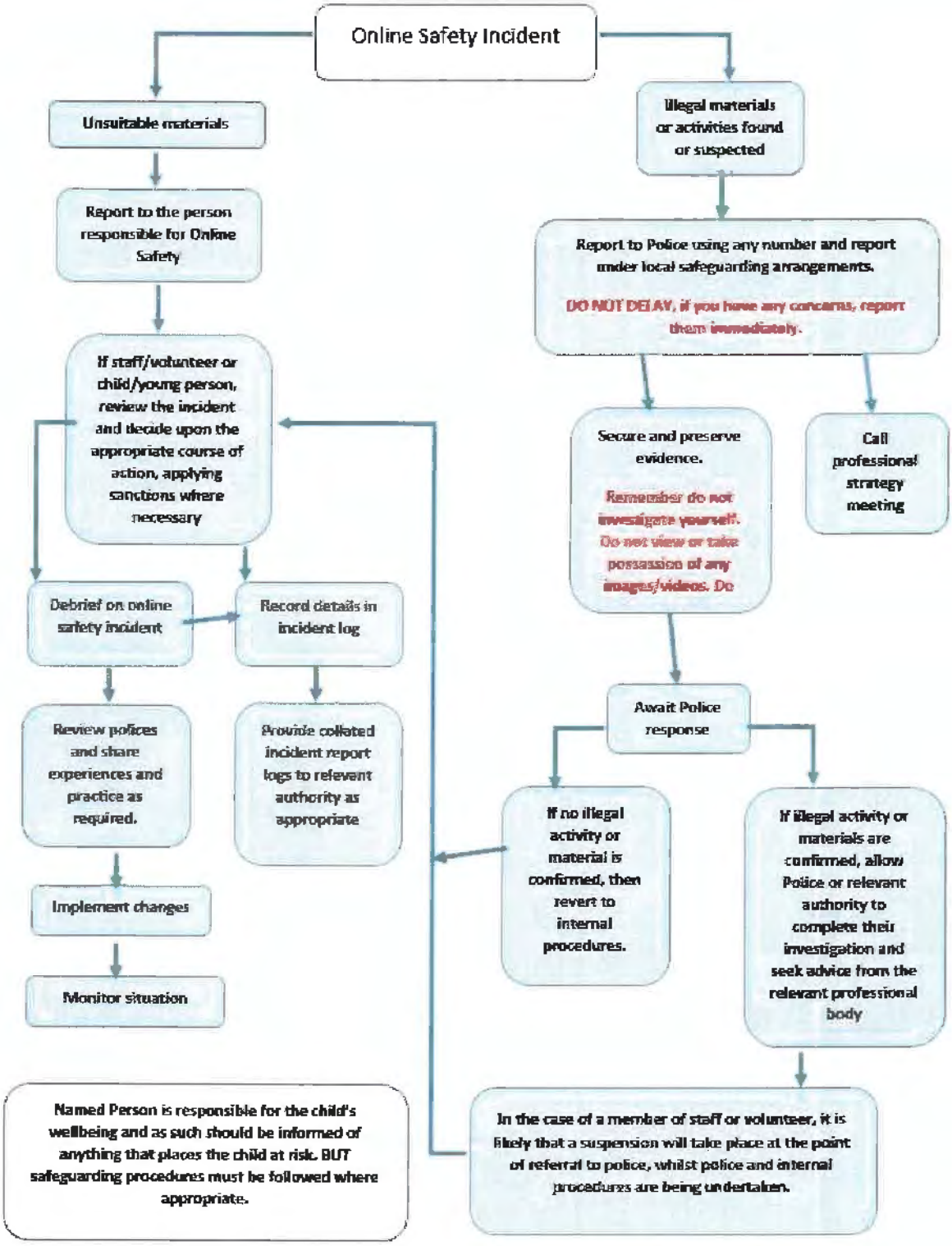
- **Grade 1:** False positive - no problem
- **Grade 2:** Inappropriate content or behaviour -
- **Grade 3:** Potentially unsafe content or behaviour
- **Grade 4:** Serious, non-urgent child safety threat
- **Grade 5:** Serious and urgent child safety threat - present or imminent danger

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). The review log Appendix B show record incidents and actions where these are not logged to our online safeguard system

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsihle or, very rarely, through deliberate misuse.

In the event of suspicion - HR guidance will be sought and:

- There will be more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- the procedure will be investigated using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. The same computer will he used for the duration of the procedure.
- the relevant staff will be given appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- the URL will be recorded of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school/academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows

Students/Pupils Incidents The decision to inform parents will be made once it has been ascertained whether the incident is deliberate or accidental, warnings may be given which could lead to further actions/sanctions. This will he decided on a case by case basis	Refer to class teacher/tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	x	x			x			
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x	x			x			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x	x			x			
Unauthorised downloading or uploading of files	x	x			x			
Allowing others to access school/academy network by sharing username and passwords	x	x		x	x			
Attempting to access or accessing the school/academy network, using another student's/pupil's account	x	x		x	x			
Attempting to access or accessing the school/academy network, using the account of a member of staff	x	x		x	x			
Corrupting or destroying the data of other users	x	x			x		x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x						x	
Continued infringements of the above, following previous warnings or sanctions	x							x
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	x	x	x		x		x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x		x	x	x	x	x

Staff Incidents In all case advice will be sought from HR/LA Lado (where applicable) and policies followed. The levels of action will be determined by the seriousness of the incident – in all cases where there is a x , the actions taken will be as appropriate or applicable, all those marked x may be considered	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X			x	x
Inappropriate personal use of the internet/social media/personal email (N.B. school staff must consider the reputational damage and links to the school)	x			x		x
Unauthorised downloading or uploading of files	x	x	x	x	x	x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x		x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x			x		
Deliberate actions to breach data protection or network security rules	x		x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x		x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x	x
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	x	x		x	x	x
Actions which could compromise the staff member's professional standing	x			x		
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy	x			x		x
Using proxy sites or other means to subvert the school's/academy's filtering system	x		x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x		x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x

Breaching copyright or licensing regulations	x		x			x
Continued infringements of the above, following previous warnings or sanctions	x		x	x	x	x

Development/Monitoring/Review of this Policy

Due to the ever changing nature of digital technologies, we will follow best practice and review the Online Safety Policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Appendix A
Giffards Primary School

Pupil Acceptable Use Policy Agreement KS1

As a school we have a responsibility to keep pupils safe and maintain the security of the technology we have. As part of this we monitor all school owned devices on and off the premises. Any incidents of misuse are reported and will be investigated

I understand that the *school* will keep me safe by monitoring my use of a school computer even if I am using a school device at home

This is how we stay safe when we use computers:

- ✓ I will ask a teacher or suitable adult if I want to use the computers
- ✓ I will only use activities that a teacher or suitable adult has told or allowed me to use.
- ✓ I will take care of the computer and other equipment
- ✓ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- ✓ I will tell a teacher or suitable adult if I see something that upsetsme on the screen.
- ✓ I know that if I break the rules I might not be allowed to use a computer

Signed (child):.....

Signed (parent): .....

Pupil Acceptable Use Policy Agreement KS2

As a school we have a responsibility to keep pupils safe and maintain the security of the technology we have. As part of this we monitor all school owned devices on and off the premises. Any incidents of misuse are reported and will be investigated.

I understand that the *school* will keep me safe by monitoring my use of a school computer even if I am using a school device at home

This is how we stay safe when we use computers:

- ✓ I will ask a teacher or suitable adult if I want to use the computers
- ✓ I will only use activities that a teacher or suitable adult has told or allowed me to use.
- ✓ I will take care of the computer and other equipment
- ✓ I will ask for help from a teacher or suitable adult if I am not surewhat to do or if I think I have done something wrong.
- ✓ I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- ✓ I am not allowed to bring in or use my own devices in school.
- ✓ I know that if I break the rules I might not be allowed to use a computer.
- ✓ I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- ✓ I will not 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 immediately report any damage or faults involving equipment or software, however this may have happened
- ✓ I will not install or attempt to install or store programmes of any type on any school device
- ✓ I will not alter any computer settings.
- ✓ I understand I am not allowed to use social media in school or on a school device even if I have a school device at home
- ✓ I will act as I expect others to act toward me:
- ✓ I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- ✓ I will not take or distribute images of anyone without their permission.

Signed (child):.....

Signed (parent): .....

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of on-line safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name _____ Student / Pupil Name _____

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, on-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed _____ Date _____

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the General Data Protection Regulation and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

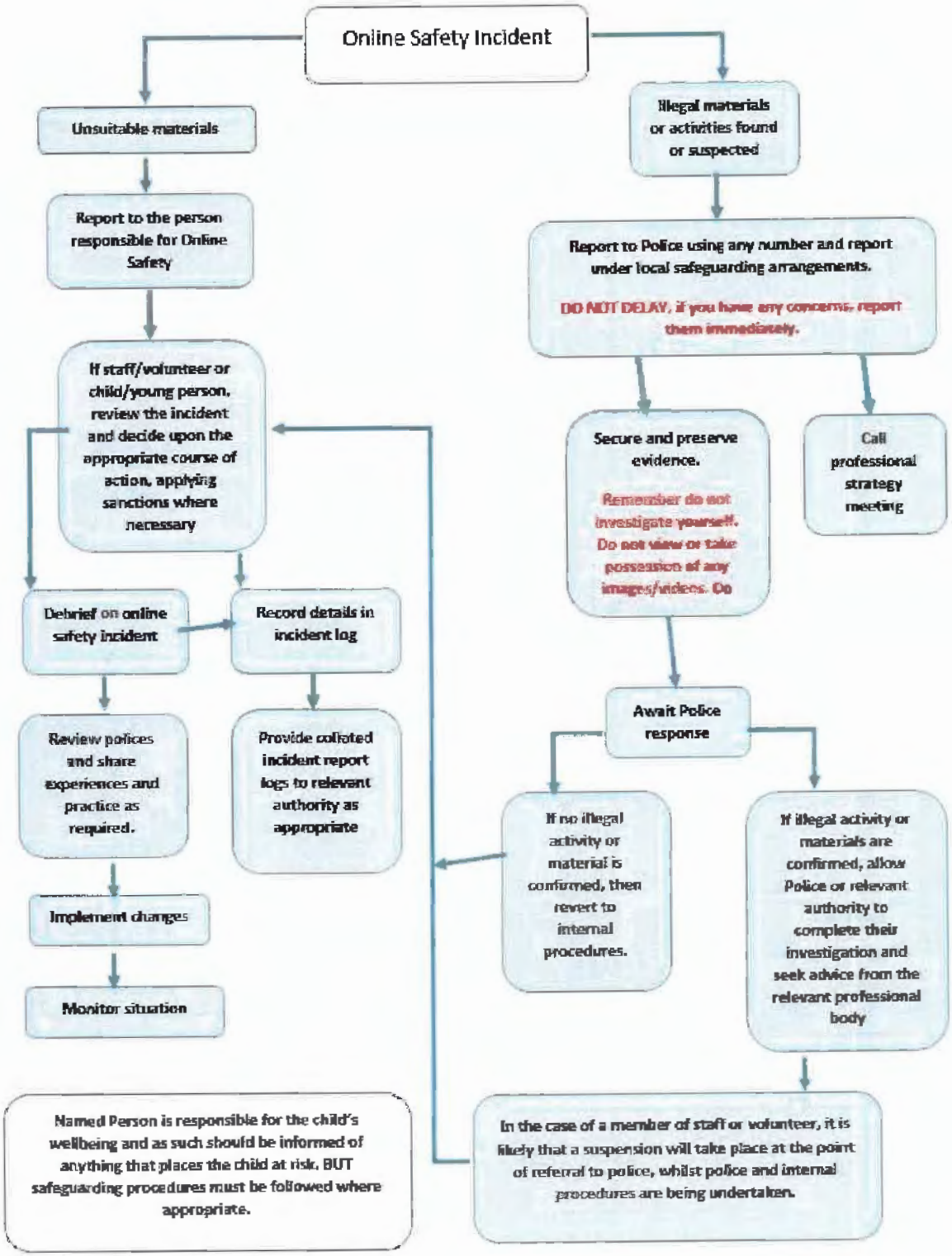
Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities.	Yes / No
As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.	Yes / No
I agree to these images being retained for educational use (e.g. these may be as images on the website/promotional information) after my child has left the school	Yes/No
I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

You may withdraw any consents given at any time by contacting the School Office and informing them of your decision.

Signed	
Date	

Appendix B


Online Safety Incident
Unsuitable materials
Illegal materials or activities found or suspected
Report to the person responsible for OnLine Safety
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Await Police response
Implement changes
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk, BUT safeguarding procedures must be followed where appropriate.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix C

Review of Incidents – that relate to staff/sit outside those reported to our pupil Safeguard System
A copy of this is kept in the admin office

Record of reviewing devices/internet sites

NB: if responding to incidents of misuse/monitoring report level 3 and above that relate to a pupil, this must be reported to our safeguard system. Staff must follow safeguarding policy.

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix D

Acceptable Use Policy Agreement (AUPA)

-this is also detailed in our Code of conduct Policy

Scope:
All Staff (and school based community user including visitors with permission to access the Internet)

Acceptable Use Agreement for Community We do not allow access to the school wifi to any external devices/visitors. This is due to the way the filtering system works, all school based devices run our monitoring software and we are unable to allow access to own devices as our system requires an additional certificate would also need to be installed to authorise access.

Installation of this certificate is strictly by permission from the Business Manager. Community users who require regular access –(e.g SCITT Students on placement at the school will be provided with a school laptop/and or their own log in to access a school based device. Can this mean they just sign the staff AUPA
Note * additions to the Juniper code of conduct AUP by the school
Addition policies linked to on line safety (social networking/mobile phones/ social networking/password policy)

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that 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 *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

ICT / online safety Acceptable Use Policy

1. Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.
All members of the school community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.
This policy is designed to ensure that all workers are aware of their professional responsibilities when using any form of ICT.
Failure to follow this policy may result in the withdrawal of access to school computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.
Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

2. Use of School Equipment/Networks Computers, Mobile Phones and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordauce with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use *(i.e. And that any devices loaned to me for professional use

will not be used by family members). Any loss, damage or unauthorised access must be reported immediately.
Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).
Any appropriate and authorised electronic communication with pupils must be through official school network, channels, systems and on school equipment.

3. Use of Email
School business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.
Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.
Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses. Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.
Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

4. Social Networks Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

Where the school operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- users should identify themselves as their official position held within the school on social networking applications eg through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

5. Personal use of school Equipment/Networks

School equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services;
- does not interfere with the user's employment or performance of professional duties or other obligations to the school;
- is of a reasonable duration and frequency;

- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- is not uses to access, send, receive or store inappropriate material; and
- does not bring the school and its community into disrepute.

Workers must notify the school of any significant personal use.
Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.
Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.
School equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines; or
- ordering of goods to be delivered to the school address or in the school's name.

6. Use of personal ICT equipment in school

Mobile Phones
It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time. Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.
Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile

telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from their line manager to do so.
Other electronic devices Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.
Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.
Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.
Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.
Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.
No pictures or videos may be taken within school or at any school related activity, on personal devises.

7. Personal social networks

The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.
The school may require the removal of content it considers inappropriate.
It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.
Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.
Individuals working in the school should not use or access social networking sites of pupils.

8. Security
The school follows sound professional practices to secure data, system programmes, email records and networks under its control.
Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:
• using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
• ensuring all devices and system access are password protected Using secured memory sticks (all laptops, memory sticks and devices used must be encrypted);
• ensuring that pupils are not exposed to any inappropriate images or web links; and
• respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
Users must not:
• use, transfer or tamper with other people's accounts and files;
• use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
• use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
• store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
• use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
• monitor or intercept the files or electronic communications of other workers or third parties;
• hack or obtain access to systems or accounts they are not authorised to use;
• use other people's log-ins or passwords; or
• breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

9. Privacy and Monitoring
At Giffards, all staff are aware that all school owned devices have monitoring/key stroke software installed. This is monitored remotely. Staff have to click to agree to this when logging on so are aware. No staff member must allow anyone to use their log in to any device.

The school respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage. However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the school reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

•when required by law;
•if there is a substantiated reason to believe that a breach of the law; or school's policy has taken place;
• if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
• if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;
• where required for compliance checks eg auditors, data protection; or

• where there are emergency or compelling circumstances.
The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).
Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.
When monitoring emails, the school will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the school) as such and encourage those who send them to do the same. The school will avoid, where possible, opening emails clearly marked as private or personal.
The school considers the following to be valid reasons for checking an employee's email:
• if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
• if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
• if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and
• if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

The school may monitor communications without notification in certain specific circumstances, including but not limited to;
• establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
• ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;
• ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
• investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the school's policy on email and internet use; and
• ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation.

10. Covert monitoring
The use of covert monitoring will only be used in exceptional circumstances, for example, where the school suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.
If the schools considers covert monitoring to be justified, this will only take place as part of a specific investigation, and will cease when the investigation has been completed.

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

•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 agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/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:.....
Appendix E

School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

If the school/academy has a mana

Responsibilities

The management of technical security will be the responsibility of the IT technician, IT support and Business Manager

Technical Security

Policy statements

The school is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- **school technical systems will be managed in ways that ensure that the school system is as safe as possible.**
  servers, wireless systems and cabling are securely located and physical access restricted
- **appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data**
- **responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff**
- **users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security**
- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- remote management tools are used by staff to control workstations and view users activity
- an appropriate system is in place (emailing the ICT technician/SBM) for users to report any actual/potential technical incident
- The provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system is decided on a case by case basis. All access rights are removed as soon as the person leaves.
- No executable files nor the installation of programmes on school devices by users is allowed.
- the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school is confirmed in this policy (no family members are allowed to use school owned equipment)

- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school/academy site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email. and learning platform).
Please see our Password policy for confirmation.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.
The school internet access is filtered for all users. Differentiated internet access is available for staff and pupils. Illegal content is filtered by our broadband provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated.
We also employ Link2ICT to alert the school to breaches of the filtering policy, which are then acted upon. This is a key stroke monitoring service and referred to above in **Technical – infrastructure/equipment, filtering and monitoring** section

.

Appendix F

Chomebook - Home Loan Agreement

Introduction

We are loaning you this chromebook for the benefit of your child in supporting and developing their education. With this chromebook your child will be able to build on and enhance their skills, knowledge and understanding.

1. The loan agreement exists between the school and the parent/carer who has signed this loan agreement.

Pupil Name:
Parent/Carer's Name & Address:

2. The chromebook will be loaned to the parent/carer for the duration of the period in which the child within their care needs to access IT for remote learning

Chromebook Serial Number .....

When your child no longer needs to work from home/self-isolate you will need to return the chromebook. We will inform you of the dates by when or on which the chromebook must be returned.

3. Should you move address from the address you have given us above, it is essential that you inform the school at the earliest opportunity.
4. You will be issued with a chromebook and power supply. These remain the property of Giffards Primary School.
5. Licensed software for use by your child is already installed on the chromebook. At no point must you open the chromebook and make changes to the inner hardware or download any other software. No personal documentation or work should be stored on the chromebook.
6. The chromebook and the connectivity equipment must not be used for any illegal and/or antisocial purpose. Included within the chromebook is software that monitors all keystrokes and we will be alerted to any inappropriate use. This is part of our safeguarding obligations.
7. There may be occasions when we need you to return the chromebook to school for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the chromebook. Giffards Primary School cannot be held responsible for the loss or damage of any data on the chromebook during this process. It is your responsibility to return the chromehook to school.
8. All technical support and maintenance must go through Giffards Primary School, please contact us if your child experiences any issues.
9. If your chromebook is stolen you must immediately report it to the police and get a crime reference number. Then immediately report this to us; we will make every effort to replace the chromebook when we are able.
10. If your chromebook is damaged/broken you will be liable for any repair costs, if your chromebook is damaged beyond repair or lost you are liable for replacement costs (new for old). We will do our best to repair the damage, if this is not possible, replacement will be on a case by case basis.

Responsibilities you have to care for your chromehook:

11. You have a responsibility to take reasonable care to ensure the security of the chromebook and connectivity equipment.

12. You must not decorate or change the external face of the equipment provided in any way, including affixing stickers.
13. Reasonable health and safety precautions should be taken when using a chromebook. The school is not responsible for any damage to person or property resulting from the chromebook or equipment loaned.
14. The school is not responsible for any costs resulting from the use of the chromebook and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.

I, the parent/carer, have read or had explained and understand the terms and conditions in the home loan agreement. I understand that by breaching the conditions the loan of the chromebook may be withdrawn by the school.

Signed _____ **Date**_____ _____

Printed Name _____

Appendix G

Remote teaching using technology and on-line devices

Remote learning platform

Only secure learning platforms will be used (such as but not limited to Google classroom/reading eggs/mathletics/TTRS/spelling shed). These are suitable for the children's age group, stage of development and ability. The school will always set up school accounts for any online platforms and the children will have a secure log in.

Livestreaming and recording sessions

Live lessons must only take place with the permission of SLT (such as during a period of school closure where remote learning was agreed necessary)

All links to live sessions must be posted in either google classroom or the schools VLE (such as Purple mash) to avoid unauthorised access or viewing

All pupils must use own log in details

No access will be allowed into live sessions from unauthorised email addresses

All live sessions must follow the protocol – see below

All live lessons must use google classroom unless permission has been given for an alternative and safe platform

Teachers need to remain alert to any risks and take appropriate actions to minimise harm.

All live lessons must be recorded to allow for monitoring for safeguarding purposes

SLT must be invited to join all classes for monitoring – this must be available at all times

All live lessons/interaction with pupils must be in accordance with this policy and be done from school equipment

Any safeguarding concerns must be logged and followed up in accordance with school policies

Pre recorded lessons

Teachers will use pre-recorded lessons so children can access at any time.

1:1 and small group live lessons

These are permitted when circumstances mean remote learning is needed or as part of educating the children in their use in school. Small group and 1:1 sessions allow children to still benefit from interventions and individualised work necessary for their education or welfare needs

All lessons must be recorded for safeguarding purposes

All protocols should be followed and staff remain alert to any risks and take appropriate actions to minimise harm.

Maintaining professional boundaries

Adults should always maintain professional relationships with children and young people.

staff must abide by our code of conduct and make it clear how you expect pupils to behave.

Staff recording or live streaming lessons, must make sure they are in a neutral area where nothing personal or inappropriate can be seen or heard in the background.

Staff should make sure that children are in a neutral area if they can be seen on camera.

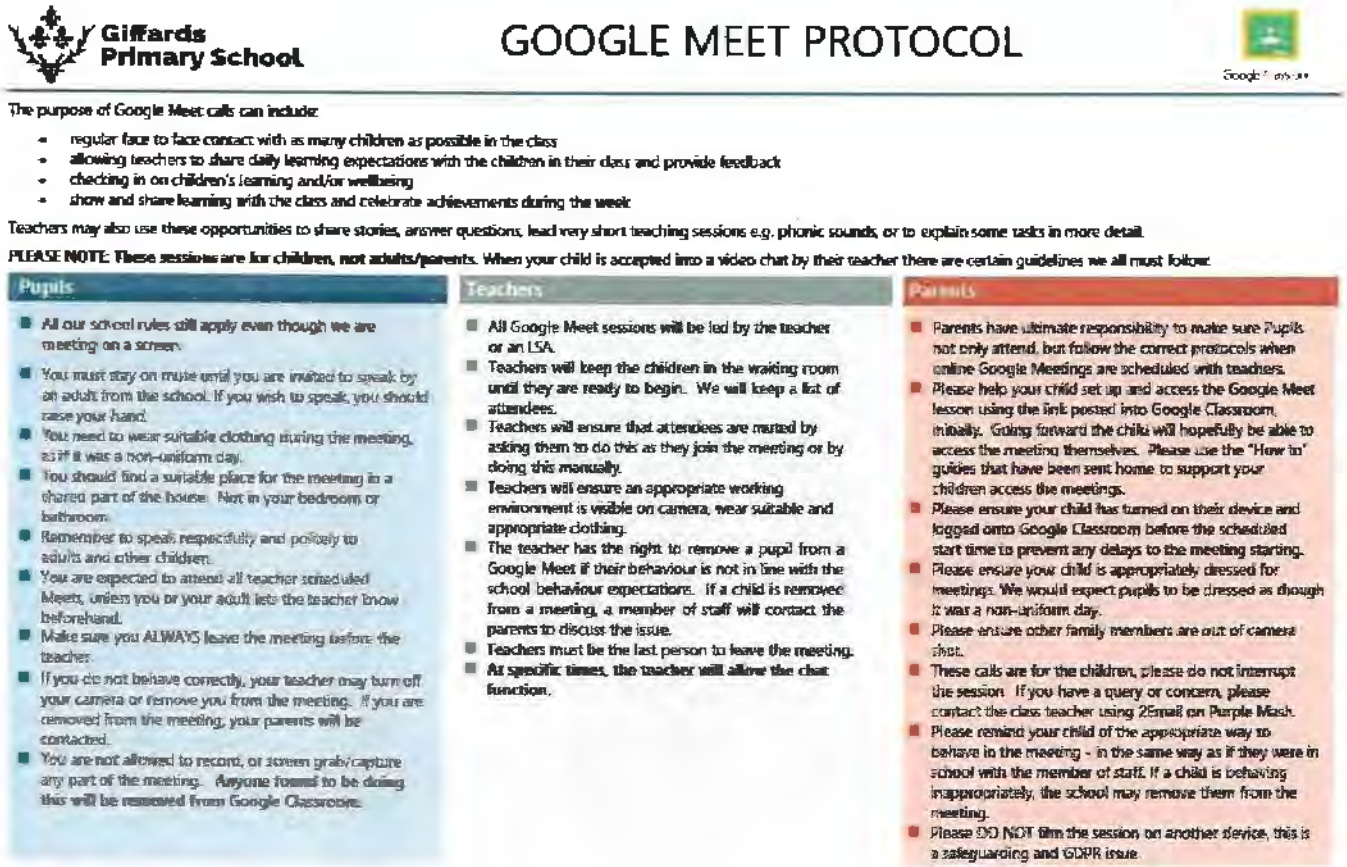
Contacting children at home

Unless there are exceptional circumstances – such as school closure/remote working, contact should only ever be made via school accounts (via email or online platforms/school phone number) never teachers' personal accounts or phone numbers.

School staff should only contact children during normal school hours, or at times agreed by the school leadership team

If no contact can be made and staff/pupils are working remotely, Staff have permission to contact families/children individually, for example to give feedback on homework. Make sure any phone calls are made from a blocked number so teacher's personal contact details are not visible.

Personal numbers must be withheld and teachers should talk to a parent in the first instance. If a parent gives permission and remains in the room, staff can talk to pupils individually.



Giffards Primary School

GOOGLE MEET PROTOCOL

The purpose of Google Meet calls can include:

- regular face to face contact with as many children as possible in the class
- allowing teachers to share daily learning expectations with the children in their class and provide feedback
- checking in on children's learning and/or wellbeing
- show and share learning with the class and celebrate achievements during the week

Teachers may also use these opportunities to share stories, answer questions, lead very short teaching sessions e.g. phonic sounds, or to explain some tasks in more detail.

PLEASE NOTE: These sessions are for children, not adults/parents. When your child is accepted into a video chat by their teacher there are certain guidelines we all must follow:

Pupils

- All our school rules still apply even though we are meeting on a screen.
- You must stay on mute until you are invited to speak by an adult from the school. If you wish to speak, you should raise your hand.
- You need to wear suitable clothing during the meeting, as if it was a non-uniform day.
- You should find a suitable place for the meeting in a shared part of the house. Not in your bedroom or bathroom.
- Remember to speak respectfully and politely to adults and other children.
- You are expected to attend all teacher scheduled Meets, unless you or your adult lets the teacher know beforehand.
- Make sure you ALWAYS leave the meeting before the teacher.
- If you do not behave correctly, your teacher may turn off your camera or remove you from the meeting. If you are removed from the meeting, your parents will be contacted.
- You are not allowed to record, or screen grab/capture any part of the meeting. Anyone found to be doing this will be removed from Google Classroom.

Teachers

- All Google Meet sessions will be led by the teacher or an LSA.
- Teachers will keep the children in the waiting room until they are ready to begin. We will keep a list of attendees.
- Teachers will ensure that attendees are muted by asking them to do this as they join the meeting or by doing this manually.
- Teachers will ensure an appropriate working environment is visible on camera, wear suitable and appropriate clothing.
- The teacher has the right to remove a pupil from a Google Meet if their behaviour is not in line with the school behaviour expectations. If a child is removed from a meeting, a member of staff will contact the parents to discuss the issue.
- Teachers must be the last person to leave the meeting.
- At specific times, the teacher will allow the chat function.

Parents

- Parents have ultimate responsibility to make sure Pupils not only attend, but follow the correct protocols when online Google Meetings are scheduled with teachers.
- Please help your child set up and access the Google Meet lesson using the link posted into Google Classroom initially. Going forward the child will hopefully be able to access the meeting themselves. Please use the "How to" guides that have been sent home to support your children access the meetings.
- Please ensure your child has turned on their device and logged onto Google Classroom before the scheduled start time to prevent any delays to the meeting starting.
- Please ensure your child is appropriately dressed for meetings. We would expect pupils to be dressed as though it was a non-uniform day.
- Please ensure other family members are out of camera shot.
- These calls are for the children, please do not interrupt the session. If you have a query or concern, please contact the class teacher using 2Email on Purple Mash.
- Please remind your child of the appropriate way to behave in the meeting - in the same way as if they were in school with the member of staff. If a child is behaving inappropriately, the school may remove them from the meeting.
- Please DO NOT film the session on another device, this is a safeguarding and GDPR issue.

Guidance and relevant documentation to support with on-line safety

Links to other organisations/documents that may be useful

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework