Gilded Hollins Community School

Online Safety Policy

Reviewed: September 2025

This policy has been written with due regard to the Equality Act 2010

Contents

1. Online Safety Policy

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's Online safety policy will operate in conjunction with other policies including those for Email Security and Etiquette Guidance, Behaviour, Anti-Bullying, Safeguarding, Child Protection, Mobile Phone, Data Protection, Image Consent form and Security.

The school will appoint an Online safety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap, and in the case of Gilded Hollins the role will be taken by the headteacher.

Our Online Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors.

The Online Safety Policy will be reviewed annually.

2. Online Safety Audit – Primary Schools

Has the school an Online Safety Policy that is approved by the Governing Body?	**Yes**
The Policy is agreed annually by the Governing Body.	
The Policy is available for staff and for parents on the school website	
The implementation of this online safety policy will be monitored by the headteacher	
The Designated Safeguarding Leads are C Burns / C Gore	
The Online Safety Coordinator is: J Martin	
Has Online safety training been provided for both pupils and staff?	**Yes**
Do all staff sign a Code of Conduct on appointment?	**Yes**
Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	**Yes**
Have school Online Safety Rules been set for pupils?	**Yes**
Are these Rules displayed in all rooms with computers?	**Yes**
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Yes
Has the school filtering policy has been approved by SLT?	**Yes**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes**

3. 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 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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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.

4. Roles and Responsibilities

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

Governors/Board of Directors

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 has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

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 (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- provides training and advice for staff

- liaises with the Local Authority

- liaises with school technical staff

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

- meets regularly with Online Safety Governor/Director to discuss current issues, review incident logs and filtering/change control logs

- attends relevant meetings of Governors

- reports regularly to Senior Leadership Team

Network Manager/Technical staff

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 Local Authority online safety policy/guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy

- the filtering policy 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 in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices

- they have read, understood and signed the staff acceptable use policy/agreement

- 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

- online safety issues are embedded in all aspects of the curriculum and other activities

- pupils understand and follow the Online Safety Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- 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 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

Designated Safeguarding Lead

Should be trained in online safety issues and be 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 pupil acceptable use agreement

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- 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 devices and digital cameras. They should also know and understand policies 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

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 in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- access to parents' sections of the website/Learning Platform and on-line student/pupil records

- their children's personal devices in the school (where this is allowed)

5. Why is internet use important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

6. How does internet use benefit education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;

- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to online learning and educational materials at home
- access to learning wherever and whenever convenient.

7. How can internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will have access to online learning tools.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

8. Policy Statements

Education –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 should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the 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 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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, Learning Platform
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/

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:

- There will be regular reviews and audits 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 (at KS2 and above) will be provided with a username and secure password by Abtec who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher/Principal or other nominated senior leader and kept in a secure place (e.g. school/academy safe)

- Abtec 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 the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- 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. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.

9. Authorised internet access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable Use Agreement'.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

10. World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the safety coordinator or network manager. This information will also be available through school's online safety system (Abtec).
- School will ensure that the use of internet-derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

11. Email

- It is the responsibility of each account holder to keep the password secure.

- For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced.
- The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Staff should never use pupils' personal email addresses under any circumstances.
- Staff must inform the Online Safety Coordinator or Headteacher if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work.
- However, you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

12. Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

13. Video conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.

14. Published content and the school website

- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

15. Social Media

Freedom of speech is a fundamental human right but it is a right that must be used responsibly. All employees should understand that they can be individually

liable for any defamatory or untrue statements that they make on any social media sites whether they have identified themselves as an employee of the school/Wigan Council or not. Furthermore, all employees must be aware that conduct online cannot always be isolated from their working life.

Employees should also be aware that if they chose to participate in any activity which compromises either their role within school or the reputation of the school as a whole then this may leave the employee open to having legal action taken against them by either the school or a third party.

Currently the law states that if an action is illegal offline then it is also illegal online therefore, all employees need to be aware that school reserves the right to take disciplinary action against any employee who breaches any of the following:

Libel/defamation

If an employee publishes either an untrue/defamatory statement or comment about another employee in school, or indeed about the school itself, which is deemed to be damaging to the reputation of either the individual or the school, then the individual or the school may choose to take legal action.

A successful libel claim will result in an award of damages against the employee.

The Acts that are likely to apply are:

- Libel Act 1843
- Defamation Acts 1952 & 1996
- Protection from Harassment Act 1997
- Criminal Justice & Public Order Act 1994
- Malicious Communications Act 1998

Copyright

Any employee placing images or text from copyrighted sources (extracts from publications, photos etc) without permission from school or otherwise is likely to breach the Copyright, Designs and Patents Act 1988. Employees should therefore not publish anything that they are either unsure about or which is deemed to be the property of school.

Disclosure of confidential information

Confidential information may include person-identifiable information for example pupil and employee records, school/Council business or records containing sensitive information and commercially sensitive information such as that relating to commercial proposals or current negotiations.

Employees should also not publish any personal data about other employees or pupils which includes photographs, videos etc

The Acts that are likely to apply are:

- Data Protection Act 1998

- The Human Rights Act 1998
- Common Law Duty of Confidentiality

Obscene material

Employees should never publish anything that is classed as obscene – this would be deemed to be a criminal offence. Obscene material is that which is designed to deprave or corrupt the audience. For the purpose of this policy 'obscene material' is that which will cause extreme offence to the school as a whole, its pupils or employees.

Publication of such material is considered a criminal offence and appropriate action will be taken.

Offensive material

Employees should never publish anything that is classed as offensive. 'Offensive', for the purpose of this policy, is material which is defamatory, racist or discriminatory on the grounds of religion, disability, gender or sexual orientation or alternatively which is designed, or is likely to, harass, victimise or bully, cause pain or distress to other employees, pupils or the school as a whole.

The Acts that are likely to apply are:

- Equality Act 2010
- Defamation Acts 1952 & 1996
- Protection from Harassment Act 1997
- Criminal Justice & Public Order Act 1994
- Malicious Communications Act 1998

Official use of social media for the school

Social media can be an appropriate and cost-effective way of making contact with residents, parents and the community, and some schools may choose to use such methods to assist in their communication processes.

Some employees may, therefore, be authorised by the Headteacher to use social media in an official capacity. The Headteacher (or senior manager, as appropriate) must ensure that the employee has read and understood this policy, before authorising them to use social media, and must also set out clear parameters and the purpose for which they are permitted to use it in an official capacity on behalf of the school.

Employees using social media in an official capacity should always disclose who they are and who they represent. They must not engage in conduct which would not be acceptable in the workplace, and must act in accordance with the provisions of this policy, and be aware of the legal aspects as outlined above.

Personal use of social media

All employees in school have a personal responsibility for their own online behaviour and activities and must ensure their use of any social media sites takes place within appropriate professional boundaries.

As a guide, the following should be adhered to by all employees:

- Employees should be cautious about identifying themselves as employees of the school or Wigan Council. This is to prevent information from being linked with the school or the Council and to safeguard the privacy of other employees. However, in certain circumstances, it may be acceptable, for example whilst using 'professional forums', which by their very nature relate to job role/profession eg LinkedIn.
- School does not expect employees to discontinue contact with their family members via any social media sites if the school starts to provide a service for them (for example if their child becomes a pupil of school) however, any information employees obtain in the course of their employment with school must not be used for personal gain nor be passed on to others who may use it in such a way.
- Employees should not have any contact with pupils' family members (unless they are related) through social media sites if that contact is likely to compromise their professional position or constitute a conflict of interest or call into question their objectivity.
- Information which employees have access to as part of their employment which may include personal information about pupils and their family, colleagues and information about school or Wigan Council must not under any circumstances be discussed in any way on any social media sites. The only exception to this may be where social media is being used for official school purposes, as outlined in paragraph 5 above.
- Photographs, videos or any other types of images of pupils, their families or images depicting school employees wearing their uniforms (if applicable) or anything which contains the school logo must not be published on any social media sites.
- School email addresses and other school contact details must not be used by employees for the purpose of setting up personal social media accounts or to communicate through such sites.
- Employees are advised to be cautious if they choose to invite work colleagues to be 'friends' on personal social media sites as this may blur the line between work and personal lives and it may be difficult to maintain a professional working relationship if for example too much 'personal' information is known. Employees are advised to ensure their 'privacy settings' are set at the appropriate level on any social media sites and to opt out of public listings in order to protect their own privacy.
- Employees should consider doing a Google search on their own name to check what information is held online about them. If any content is found that they would prefer not be accessible, they can request that this is removed, by

asking the person who uploaded it if the person is known by them, or if appropriate, by using the “report abuse” facility within the particular site.

- Employees are advised to keep their log-in details and passwords confidential at all times in order to ensure no other person can access their accounts.

Online contact with children and young people

There is a concern that social media sites may increase the potential for sexual exploitation of children and young people or provide the opportunity for ‘grooming’ to take place. It is also possible that employees who work with children may be at risk of false allegations being made against them.

It is therefore vital that employees who use social media take appropriate steps to protect themselves from such allegations, maintain appropriate boundaries, exercise their professional judgement and avoid any contact that may lead to their intent and motivations being questioned.

As a guide, the following should be adhered to by all employees:

- Employees should not share personal information with pupils
- Employees must not have contact through any social media sites with any pupil whether from their current school establishment or another unless that pupil is a family member.
- Should a pupil attempt to contact an employee via any social media sites then this should be reported to the Headteacher immediately.
- Employees must decline all ‘friend requests’ they receive from any pupil or young person to whom they have acted in a position of trust whether in their current school establishment or another.
- Employees who leave employment from their current school must not contact pupils by means of social media sites if this compromises their professionalism or objectivity.
- Employees should be cautious when using such sites at Twitter or other online chat rooms as it may be difficult to ascertain to whom they may be chatting.

Online bullying and harassment

Social media can have potential dangers and drawbacks as both adults and children have found themselves the target of online abuse, harassment and bullying which is often referred to as ‘cyber bullying’ which includes:

- Name calling
- Malicious comments
- Exclusion
- Intimidation
- Spreading of rumours
- Bombarding with unwanted messages

Cyber bullying can have a significant impact on health and wellbeing and will not be tolerated. Should any employee feel they have been a victim of cyber bullying this should be reported to the Headteacher in the first instance. If it is

the Headteacher who is the victim concerns should be raised with the Chair of Governors.

16. VLN

- Parents will be asked to return and sign a consent form for their child's use of the VLN (for example, Seesaw).
- Parents, staff and governors will also be asked to return and sign terms of acceptable use for the VLN.
- Photographs of pupils will only be published on Gilded Hollins interest pages, Seesaw, Twitter or any other social media site with written permission from parents and carers.
- Work can only be published with the permission of the pupil.
- Children will have access to their VLN at home via a personal password.

17. Remote learning for pupils

We will provide access to appropriate remote learning for pupils that are not able to attend school so that no-one need fall behind. In the following points, an outline of the provision will be made, and some guidance given on the role of pupils, teachers and parents.

The governors and senior leadership team at Gilded Hollins Primary School are fully aware that these are exceptional times and that this document seeks to inform and guide families and not impose expectations. Each family is unique and because of this, should approach home learning in way which suits their individual needs. We realise that the circumstances that cause our school to close will affect families in a number of ways. In our planning and expectations, we are aware of the need for flexibility from all sides:

• parents may be trying to work from home so access to technology as a family may be limited;

• Parents may have two or more children trying to access technology and need to prioritise the needs of older children studying towards GCSE/A Level accreditation;

• systems may not always function as they should.

Teacher expectations

• Teachers will plan lessons that are relevant to the curriculum focus for that year group and endeavour to supply resources to support tasks for home learners.

• All communication will take place through Seesaw. Parents may only contact teachers between the hours of 8am and 5pm. Teachers will endeavour to answer queries within 48 hours.

• Work for the day in English, Maths and other subjects will be posted on Seesaw by 9.00am.
• Teachers will post video links to be used by children in English and maths each day. Children should refer to them before completing their work. These video links may be from a reputable, accredited provider but will primarily be recorded for Seesaw by the teacher to ensure familiarity and continuity.
• Worksheets / activities will be posted on Seesaw to be completed remotely by children. This work should, where possible, be completed before the end of the school day and returned remotely through Seesaw.
• Teachers will provide feedback on work completed as appropriate. This may be a comment, correction or remote acknowledgement.
• Children should read daily and complete planners as is expected practice throughout school. Parental completion of planners should be submitted through Seesaw to be monitored by the class teacher .
• A curriculum map, which details subjects other than English and maths, may be referred to on the school website and used by parents to enhance learning.
• Teachers will respond promptly, within reason, to requests for support from families at home. This should be done via Seesaw.
• Should a staff member require support with the use of technology, it is their responsibility to seek this support in school and Senior Leaders will ensure that support is given promptly.

Family (pupil/parent/guardian) role
• Where possible, it is beneficial for young people to maintain a regular and familiar routine. Gilded Hollins Primary School would recommend that each 'school day' maintains structure. A suggested timetable will be put on the relevant class web page as a guide during a closure period.
• If a class bubble is isolated, the children will be sent home with their class reading book in addition to an exercise book – this is so that work that children complete at home can be kept safe, ideally in their exercise books, and can be brought back to school when safe to do so.
• Should anything be unclear in the work that is set, parents can communicate with class teachers via Seesaw or by contacting the school office.
• We would encourage parents to support their children's work, by viewing the work set together, and then making appropriate plans to complete the work. This can include finding an appropriate place to work and, to the best of their ability, supporting pupils with work encouraging them to work with good levels of concentration.
• Every effort will be made by staff to ensure that work is set promptly on appropriate platforms, but school cannot guarantee that the chosen platforms will work on all devices. Should accessing work be an issue, parents should contact school promptly and alternative solutions will be made available (e.g. paper copies of work etc). These will be discussed on case-to-case basis.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

18. Use of mobile phones in school

Mobile phones are not permitted into the main body of the school building. Lockable cupboards are situated in the staffroom and outside the school office, and staff lock their phones in these by 8.30am. Phones can then be accessed at break time and 3 lunchtimes before being locked away again. Phones are not to be taken out of the staffroom during the school day. All staff are expected to adhere to this rule. The staffroom is a 'No pupil zone'. This is to prevent those pupils carrying out recycling, or collecting cool packs, entering a room where staff are using mobile phones. Additional signs will be displayed in school informing visitors and staff that Gilded Hollins has 'No Mobile Phones' policy.
In the same vein, smart watches should not be used to access emails, text messages, social media during the school day.

Emergency contact: The school's main switchboard number is the main emergency contact number for staff during school hours.

Staff and school visits: Staff and other adults who have DBS clearance directly through Gilded Hollins are permitted to take their own mobile phones stored securely in bags or pockets. This is only for possible occasions when emergency internet access is required, or if the member of staff requires information (or indeed a signal) that may not be available from the school phones. Members of staff and other adults with a Gilded Hollins DBS must only use their personal mobile phones in the above scenarios. If it is the case that a personal mobile phone has to be used the individual must ask a colleague on the visit to witness the phone being used. Personal phones should not be taken out of pockets or bags to check for messages or emails, or used to take photographs of pupils. Photographs should be taken with a school ipad. Pupils will be directed to speak to the trip leader should they witness personal mobile phones being used.

Parents accompanying school visits: Parents accompanying pupils on trips out of school must hand over their phone for safekeeping in school before joining the trip unless they have received DBS clearance directly from Gilded Hollins. This expectation will be clearly outlined in letters home requesting parent helpers for visits. All letters seeking permission from parents / carers to take pupils out of school for a visit will contain a slip requesting two emergency contact numbers. This will provide the office with contact details for adults who are accompanying trips should they be required in an emergency. Staff members will ensure that emergency numbers are taken on all trips out of school so that parents can be reached in an emergency.

Visitors to school / volunteer helpers: A second lockable cupboard is located outside the school office. This will be used for the mobile phones of any adult about to progress beyond the office into the school. This includes volunteers

listening to readers, parents given tours of the school prior to their child enrolling at Gilded Hollins, Governors visiting their class, workmen entering during the day, peripatetic visitors, music service, and sports coaches. This list is not exhaustive.
No mobile phones will be permitted into areas accessed by pupils. Efforts will be made to ensure that the school office is manned at all times so phones left for safe keeping can be readily retrieved.

Parents at the end of the school day: Parents who call into school after the end of the school day to meet their child's class teacher will not be asked to hand over their mobile phones as they will be directly accompanied to and from their child's classroom by the class teacher. For evening meetings such as Parents' Evenings, Full Governors and Committees, workshops covering topics such as phonics, SATs or residentials, Friends of Gilded Hollins, visitors will not be asked to hand over their mobile phones.

Residential visits: Staff accompanying pupils on residential visits may take their own mobile phones for the duration but must only be used following the guidance outlined above. Personal mobile phones must not be used to take photographs of children at any time. Staff may use their own phones to call home from their room in an evening or may walk to an area away from the residential centre to pick up a signal to call home (Low Bank Ground). If a parent is asked to accompany their child on a residential (e.g. for medical reasons) identical rules to those of school staff will apply. The parent must not use their phone while children are present and must not take photographs using their phone, even of their own child. Parents will be asked to agree to these restrictions in writing.

iPads and laptops: All staff laptops and iPads must be secured with an individual login for each member of staff. This is to prevent access by anyone else when the equipment is away from school. All passwords must be passed to the school office for secure storage. Staff using iPads agree to take full responsibility for the contents of their iPad. Any staff iPad may be subject to a spot check by a member of the Senior Leadership Team to ensure appropriate usage. Spot checks will be undertaken on a purely random basis.

Assemblies and School Performances: At the start of the year parents are asked to read and sign Gilded Hollins' Photographic Policy granting or withholding permission for photographs to be taken in a range of circumstances. During class assemblies or performances when parents are present the headteacher or deputy headteacher will inform the audience if photographic permission has been granted for everyone on stage. If that is the case, then parents will be permitted to take photographs during the performance. However, they will be warned that no photographs containing children other than their own should be uploaded to social media. If any child in the production does not have

the required photographic permission, then no full group / cast photographs may be taken at all. Photographs of individual children must wait until the end of the performance.

19. Use of digital and video images

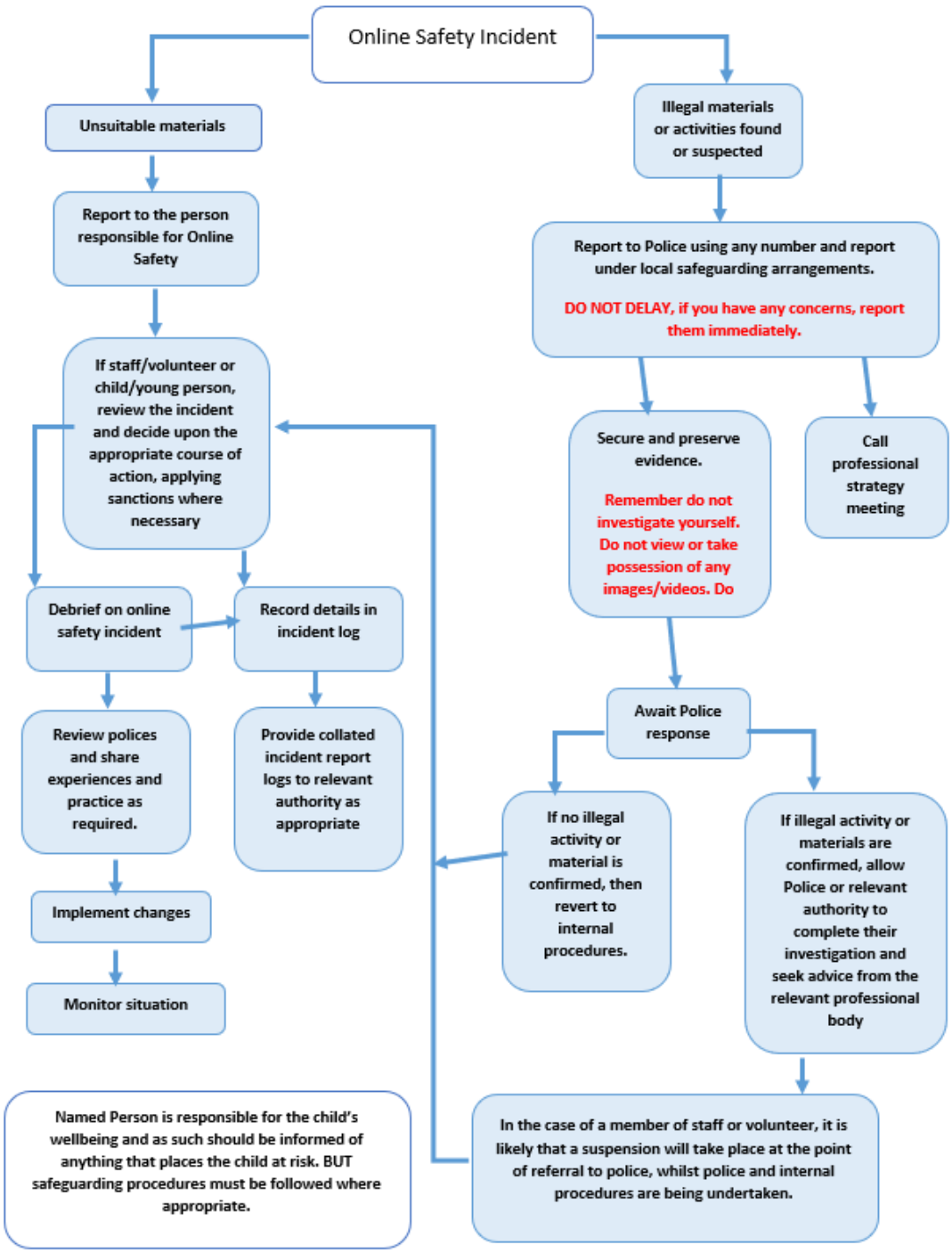
The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 pupils are published on the school website/social media/local press
- 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 other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

20. Responding to incidents of misuse

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 Flowchart for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
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
Implement changes
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.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
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
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.

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 irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure 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. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL 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/Academy Group or national/local organisation (as relevant).
    - 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.**

21. Protecting Personal Data

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

22. Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wigan LEA can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

23. Communication of policy

Pupils

- Rules for internet access will be discussed and displayed in all classrooms.
- Pupils will be informed that internet use will be monitored.
- Pupils will be taught about internet safety and cyberbullying through a number of means. These will include: through ICT lessons, assemblies, PHSE and circle time links, and through participation in national events such as Safer Internet Day.
- Posters reminding pupils of internet safety and cyberbullying will be displayed around school.

Staff

- All staff will be given access to the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.

24. Online Safety Rules

These Online Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made under the supervision of an adult.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Our School - - Online Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the online Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by full pupil names.

Parent's Consent for Internet Access

I have read and understood the school online safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**

Please print name:

Please complete, sign and return to school

25. Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's online safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Accepted for school: …….. Capitals: