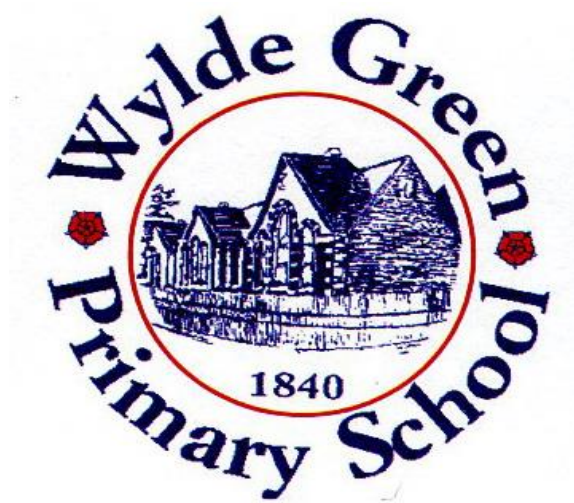


WGPS E-SAFETY POLICY



Policy lead:	Hannah Ambrose
Link Governor:	Darren Harris
Sub-committee:	RASP
Date of last review:	June 2025
Date for next review:	June 2026

Statement of intent

Wylde Green Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

What is E-safety?

E-safety encompasses internet technology and electronic communications, such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The E-Safety Policy will operate in conjunction with other school policies including but not limited to: Safeguarding policy, KCSiE 2024, Health and Safety, Behaviour & Relationships policy, Data Protection Policy and our curriculum statement.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and WGPS and to personal devices owned by adults and young people while on the school premises.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

Related Documents

This policy operates in conjunction with the following school policies:

- Acceptable Use Policy for Adults
- Acceptable Use Policy for Young People (Key Stage 1 and 2)
- Data Security Policy
- Behaviour & relationships Policy
- Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)

Roles and Responsibilities

Head Teacher

The Head Teacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing body to update this policy on an annual basis.

DSL

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and I.T. technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing body about online safety termly.
- Working with the Head Teacher and governing body to update this policy on an annual basis.

E-Safety Coordinator

It is the role of the E-Safety Coordinator to take responsibility for day to day issues regarding e-safety. These are, but not limited to:

- Ensuring staff are aware of procedures to be followed in the event of an e-safety incident taking place.
- Provide training and advice for all staff relating to e-safety.
- Liaise with the Local Authority, regarding e-safety updates or concerns.
- Oversee monitoring and recordkeeping of e-safety events
- Ensure technical staff keep monitoring and filtering systems up to date.
- Monitor CPD for themselves and other staff to make sure e-safety roles can be fulfilled.

I.T. Technician

The I.T. technician is responsible for:

- Providing technical support in the development and implementation of the school's Online Safety Policy and procedures.
- Implementing appropriate security measures as directed by the Head Teacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Head Teacher to conduct annual reviews of this policy.

Staff members

All members of the school have certain core responsibilities within and outside the school environment. They should have an up to date awareness of e-safety matters, policy and practices.

- They have understood and signed the school Staff Acceptable Use Policy
- They report any suspected misuse to the Head Teacher/DSL/Class Teacher/E-Safety Co-ordinator
- Digital communications with pupils (email/website) are professional and only carried out using official school systems.
- E-safety is embedded in all school activities and the curriculum.
- Use of I.T. is monitored carefully in school, including handheld devices such as camera and phones.
- Internet research is monitored with children guided to pre-checked sites and are aware of procedures for dealing with and unsuitable material.
- Pupils are aware of and following the Pupil Acceptable Use Policy.

Pupils

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents/Carers

Parents and Carers play a crucial role in ensuring children understand the need to use the internet and mobile devices in an appropriate way. We ask Parents/Carers to maintain appropriate boundaries and avoid behaviour, during their use of the internet and other communication technologies, which may be misinterpreted by others, can cause offense to any member of the school community, put at risk child safety or bring the school's reputation into disrepute.

- Parents' attention will be drawn to the school E-safety Policy in an e-safety leaflet, newsletters, the school prospectus and on the school website.
- The school will maintain an online list of e-safety resources for parents.
- The school will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Head Teacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct. If the concern is about the Head Teacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Head Teacher and I.T. technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour & Relationships Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head Teacher contacts the police. All online safety incidents and the school's response are recorded by the DSL.

Responding to incidents

- Any suspected illegal activity will be reported directly to the police. The I.T. technician will also be informed to ensure that the Local Authority can provide appropriate support for the school.

- Complaints concerning activity that occurs outside the normal school day should be referred directly to the Head Teacher.
- Breaches of this policy by staff will be investigated by the Head Teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by the DSL/Head/Deputy Head Teacher.
- Minor pupil offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking our behaviour policy.
- More serious pupil policy breaches must be reported to the DSL or e-safety coordinator and action taken in line with our Behaviour & Relationships and Safeguarding policies. There may be occasions when the police must be involved. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- The Education and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Behaviour Policy.

While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or social networking sites, are becoming more frequent. As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying. The school's school Behaviour & Relationships Policy will address cyberbullying. Cyberbullying will also be addressed in Computing, P.S.H.E. and other relevant lessons and is brought to life through activities. As with other whole school policies, all staff and young people will be included and empowered to take part in the process. Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Behaviour & Relationships Policy and the Safeguarding Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.

The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Physical Environment / Security in school and the WGPS

We endeavour to provide a safe environment for the whole community and we review both physical and I.T. security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly.
- Central filtering is provided and managed by the I.T. technician and the DSL and approved by Head Teacher following a request. All staff and pupils understand that if an inappropriate site is discovered it must be reported to the DSL/e-Safety co-ordinator who will report it to the I.T. Technician to be blocked. All incidents will be recorded in the e-safety log for audit purposes, (sample page below).
- Requests for changes to the filtering will be directed to the DSL and e-Safety co-ordinator in the first instance who will forward these on to I.T. technician if appropriate. Change requests will be recorded in the e-Safety log for audit purposes.
- The school and WGPS use *ClassroomCloud* on school owned equipment to ensure compliance with our Acceptable Use Policies.
 - Pupils use is monitored by the I.T. Technician, DSL and Computing lead
 - Staff use is monitored by the I.T. Technician and DSL .
- Staff are issued with their own username and password for network access. This must not be shared with any other person. (Generic names / passwords must not be used).
- Visitors / Supply staff may be issued with temporary ID's when logging onto the school system using Google Drive.
- Key stage one and two pupils use their own individual login ID to log into their Google Drive.

Social Media, including Facebook and X (Twitter).

Facebook, X and other forms of social media are increasingly becoming an important part of our daily lives. The school communicates with Parents and Carers via email and text messaging. The staff are responsible for all postings on these technologies. Furthermore, school educational activities including trips and sports competitions are published on X using the School's X handle. No names of children are published and prior permission (*when children join the school parents sign a consent form*) from parents are obtained for publishing images of their child.

Staff, governors, pupils, parents and carers are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Furthermore, staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever. Also, staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Wylde Green Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so
- Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school 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 or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Mobile / emerging technologies

Technology is evolving constantly as new programmes, software and devices are developed and released. It is vital that staff, pupils and parents are aware of their potential and their risks.

- Emerging technologies will be evaluated for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The SLT should note that technologies, such as personal hand held devices with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.
- Personal Mobile phones must not be used when children are in the vicinity.
- Staff will not use personal mobile phones to communicate with children.
- Staff are provided with laptops and iPads for educational use and their own professional development. Staff understand that the Acceptable Use Policies and monitoring systems apply to this equipment at all times.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment such as iPads for this purpose.
- Pupils from years R-5 are not allowed to bring mobile telephones to school.
- The Education and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Staff will not use personal social media on school devices during school time.

E-mail

Our e-mail system is provided, filtered and monitored by the I.T. technician and DSL and is governed by Birmingham City Council E-mail Use Policy

- Staff may be given an e-mail address and understand that this must be used for all professional communication.
- Pupils may be provided with a general school / class e-mail address that can be used for educational purposes.
- Everyone in the school / WGPS community understands that the e-mail system is monitored and should not be considered as private communication
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment must be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.
- Everyone in the school / WGPS community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible.
- The forwarding of chain letters is not permitted.
- Staff must not communicate with any pupil by e-mail, (or other personal messaging system) except through the school e-mail system.
- Any content within an email which refers to pupils must be sent via a school email address rather than a personal email address.

Published content

The Headteacher takes responsibility for content published to the school web site, but delegates general editorial responsibility to the website link member of staff and the website management company. Teachers are responsible for the editorial control of work published by their pupils.

- The school website complies with the following statutory DfE guidelines for publications:
 - *What maintained schools must publish online?*
- The point of contact on the website is the school address and telephone number. The school uses a general email contact address: enquiry@wyldegrn.bham.sch.uk. Home information or individual email identities will not be published.
- WGPS holds the copyright of any material published on the school website, or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- WGPS encourages the use of e-mail to contact the school via the school office.
- WGPS does not publish any contact details for the pupils.
- Photographs used on the website will not allow named identification of individuals. Their inclusion must be carefully considered by staff.

Digital Media

- Pupils' full names will not be published outside the school / WGPS environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Pupils understand that they must have their teacher's permission to make or answer a video conference call and their use will be supervised.
- A consent form for publication of pictures will be sent to parents / carers for agreement.
- Permission from staff, or other adults within school, must be agreed before any images or video are published or distributed of them.

Educational Use

School / WGPS staff model appropriate use of I.T resources including the internet.

- All activities using I.T and the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material. (NB especially for sites such as Youtube).
- Where appropriate, links to specific websites will be provided instead of open searching for information.
- Pupils will be taught how to conduct safe searches of the internet.
- Teachers will be responsible for their own class management when using I.T. equipment and will periodically remind pupils of our Acceptable Use Policies.
- Staff and pupils will be expected to reference all third party resources that are used. All downloads, copies must be legally carried out.

E-safety training

WGPS has a programme of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- There is an induction process and mentoring available for new members of staff.
- Educational resources are reviewed, including for e-safety issues, and disseminated through staff meetings and training sessions
- E-Safety is embedded throughout the school curriculum and visited by each year group
- Pupils are taught how to consider the accuracy of information found on the internet

E-Safety and Teaching and Learning

The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. To ensure e-safety across the curriculum:

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- E- Safety delivery will be mapped across the curriculum to ensure full coverage.

Staff should guide pupils in:

- On-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- The effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.
- Being critically aware of the materials they read and shown how to validate information before accepting its accuracy. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Data Security / Data Protection

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

Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines. If data is sensitive encryption will be used by staff if they need to take personal data off the WGPS site. Users must gain permission before taking highly sensitive data off site.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office

Equal Opportunities and Inclusion

All teaching and non-teaching staff at Wylde Green Primary School are responsible for ensuring that all pupils, irrespective of gender, ability, ethnicity and social circumstances, have access to the whole curriculum and opportunities to make the greatest progress possible in all areas of the curriculum while in our school, including using I.T.

Inclusion is achieved through analysis and assessment of all our children's needs, this may require additional monitoring and supervision of e-safety for some individual children.

Any parental request that their child does not have access to I.T. or the Internet will be referred to the Headteacher. Such requests made on religious grounds will be accepted. Other requests will be considered by the Headteacher on a case by case basis bearing in mind the requirement to teach I.T. as part of the National Curriculum.

The governors will ensure that:

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

ACCEPTABLE USE POLICIES FOR WYLDE GREEN PRIMARY SCHOOL / WGPS

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers, they may also arise through the use, for example, of games consoles and mobile phones.

There is an expectation that schools will have in place appropriate policies and strategies to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

Part of the apparatus for promoting e-safety is a set of Acceptable Use Policies (AUPs). The enclosed drafts are intended to be read as notes towards the contents of our schools' acceptable use policies; they are intended to act as a skeleton for a school's policies; perhaps to form the basis of the text which appears on screen when a user logs on to a school's learning platform or VLE. They could also be used and have been used as teaching aids for school age learners and adults.

1. AUP for younger learners in KS1
2. AUP for learners in KS2 and upwards
3. AUP for all adults working with I.T. in WGPS
4. Agreement signed by all staff who have allocated laptops

There is not an AUP for children in Foundation Stage.

The key principles of the AUP should also be shared with parents and carers and provide a shared expectation of the behaviours children must adopt whenever, and wherever, they are using technology.

Acceptable Use Policy for Learners in KS2

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

I agree that I will:

- ✓ always keep my passwords a secret
 - ✓ only visit sites which are appropriate to my work at the time
 - ✓ work in collaboration only with friends and I will deny access to others
 - ✓ tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
 - ✓ make sure all messages I send are respectful
 - ✓ show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
 - ✓ not reply to any nasty message or anything which makes me feel uncomfortable
 - ✓ not give my mobile phone number to anyone who is not a friend
 - ✓ only email people I know or those approved by a responsible adult
 - ✓ only use email which has been provided by school
 - ✓ talk to a responsible adult before joining chat rooms or networking sites
 - ✓ always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
 - ✓ always check with a responsible adult and my parents before I show photographs of myself
 - ✓ never meet an online friend without taking a responsible adult that I know with me
-
- ❖ I know that once I post a message or an item on the internet then it is completely out of my control.
 - ❖ I know that anything I write or say or any website that I visit may be being viewed by a responsible adult

Agreed by : _____ Dated : _____

Acceptable Use Policy for adults working with ICT at Wylde Green Primary School

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

I agree that I will:

- only use personal data securely
- implement the schools policy on the use of technology and digital literacy
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc...
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the e Safety Coordinator
- ensure that videoconferencing is supervised appropriately for the learner's age
- read and sign the acceptable use policy
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied E-safety guidance appropriately

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - pornography (including child pornography)
 - promoting discrimination of any kind
 - promoting racial or religious hatred
 - promoting illegal acts
 - breach any Local Authority/School policies, e.g. gambling
 - do anything which exposes children to danger
 - any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law
- I accept that my use of WGPS and Local Authority I.T. facilities may be monitored and the outcomes of the monitoring may be used.

AUP agreed by : _____ Dated : _____

Agreement for Loan of Laptop Computer/iPads

[Staff's Name] and **Wylde Green Primary School** hereby agree as follows:

- 1 The laptop computer/iPad identified below shall be loaned to **Staff's Name** for his / her personal use. The loan shall terminate when [Staff's Name] ceases to be employed at **Wylde Green Primary School**, unless the School deems the loan to be terminated by breach of conditions in which case it will terminate forthwith. On the termination of the loan, the laptop computer/iPad shall be returned to the School.
 - 2 **[Staff's Name]** has not previously been in receipt of any computer equipment funded by Government grants.
 - 3 The laptop computer/iPad is not covered by insurance, but **Wylde Green Primary School** will make good any loss or damage whilst on school property. **[Staff's Name]** is to ensure she has adequate home insurance if the laptop/iPad is to be taken off site, in the event of loss or damage. **[Staff's Name]** is aware of the level of risk s/he undertakes by virtue of this provision.
 - 4 **[Staff's Name]** agrees to abide by Birmingham City Council and **Wylde Green Primary School's** policies in respect of
 - observance of requirements in respect of the Data Protection Act 1998 (see <http://www.bgfl.org/services/editdata> and <http://www.dataprotection.gov.uk/>), in particular the specific requirements under the Act imposed by the School's registration with the Information Commissioner.
In practice this means that teachers should refrain from using, on their laptops, information about identifiable individuals: if they do (eg assessment data exported from SIMS or Facility), they need to exercise great care in keeping their work under a secure user password, which is not known to other users of the laptop such as family members.
 - acceptable use of computer networks (including the Internet and the Birmingham Grid for Learning) (see <http://www.bgfl.org/services/lft/resp-netpolicy.htm>)
 - health and safety of **[Staff's Name]** or any other individual (see <http://www.bgfl.org/services/lft/resp-health.htm>)
- [Staff's Name]** will in addition take all reasonable steps to ensure that any other user of the laptop/iPad will also abide by these requirements.
- 5 **[Staff's Name]** agrees to pay any telephone or telecommunication charges incurred in connecting the laptop/iPad computer to private or public networks, except in the case of connection to the Local Area Network of any school in connection with professional duties. **[Staff's Name]** understands that the supply and use of consumables used at home are the teacher's responsibility.
 - 6 In the event of the laptop/iPad requiring repair, **[Staff's Name]** will return the laptop computer/iPad to **Wylde Green Primary School** for collection and repair by the supplier and will arrange for such collection and repair. **[Staff's Name]** undertakes not to attempt any such repair him/herself. In this event, **[Staff's Name]** agrees that software repair may be limited to restoration of the computer's original software image and therefore that responsibility for regular backup of data and validation of backups rests with **Staff's Name**. **Wylde Green Primary School's** ICT staff will facilitate such backups and validation, for example by appropriate connections to the school's Local Area Network.
 - 7 **[Staff's Name]** undertakes not to install any software on the laptop computer /iPad without the written sanction of **Wylde Green Primary School**. **[Staff's Name]** further undertakes not to install any Internet Service Provision (other

than that provided with the laptop computer/iPad) without the written permission of **Wylde Green Primary School**, which shall not be granted without consultation with appropriate officers of Education IT Services. **[Staff's Name]** will ensure that the laptop/iPad anti virus software is regularly updated and will cooperate in maintaining the **Wylde Green Primary School** anti-virus policy. **[Staff's Name]** will produce the laptop/iPad if requested by **Wylde Green Primary School** for anti-virus checking and updating if required to do so.

- 8 **[Staff's Name]** and **Wylde Green Primary School** agree that the teacher may use the laptop computer/iPad for any purpose s/he wishes, provided solely that it shall not result in personal financial gain for the teacher or any of his/her family or associates, but the expectation shall be that such purpose shall primarily be for the teacher's personal and professional development in connection with her/his duties in the school, and that both parties shall collaborate in recognising what activities might produce outcomes beneficial to both the teacher and the school. To this end, **Wylde Green Primary School** will endeavour to provide any training mutually agreed to be necessary. Both parties agree to provide any information requested by Birmingham City Council officers, the Department for Education and Skills, the Office for Standards in Education, National College of School Leadership, or other comparable agency, in investigating the effectiveness and value for money of the Laptops for Teachers Initiative.

Schedule of Loan:

Laptop Computer/iPad – Make:

Model:

Serial number:

School Inventory Reference:

Teacher's name: **[Staff's Name]**

Post: **Teacher**

Signature.....Date.....

Authorised by **Mr Richard Hamilton-Martin** on behalf of Wylde Green Primary School

Signature.....Date.....

Returned and Checked by: (print name)

Reason for return:

Signature.....Date.....

Monitoring ICT / Internet use - Appendix to Wylde Green Primary School e-safety policy

It is a requirement at Wylde Green School that I.T., Internet and E-mail usage is monitored to ensure compliance with our, and Birmingham City Council's, Acceptable Use Policies (AUPs).

This is achieved through the use of third party monitoring software – ClassroomCloud. This software helps us to safeguard staff and pupils, highlight local risks and challenge risky or inappropriate behaviour. This software is managed at a Senior Leadership level with appropriate policies and processes in place to deal with any issues that are raised.

The Software

ClassroomCloud compares words or phrases that are typed on the keyboard or displayed on the screen with a series of dictionaries containing known inappropriate text. When it finds a match, one or more actions may occur including: recording the date and time, the logged on user, the computer name, taking a screen shot, displaying a warning even sending an e-mail alert to one or more nominated people.

It also keeps a historic log of the information collected allowing investigations of ongoing issues as well as track behaviour changes over time.

Managing the process

The following users manage the process:

The DSL in line with our e-safety policy. Responsible for monitoring data and identifying trends and issues; recommending changes to the system configuration; responding to potential child protection issues; recording the monitoring that has taken place.

Head Teacher or deputy Head Teacher. To assist with the monitoring and review process.

A technical lead responsible for: installation and configuration; managing requested changes; documenting all changes to the system.

Managing the information

ClassroomCloud captures may contain inappropriate, upsetting or illegal content. All users must be aware of this prior to accessing the system and care must be taken to ensure that other members of the school / WGPS are not exposed to this content.

Under no circumstances should this kind of content be distributed or transferred by any means (electronic or otherwise) without seeking guidance from Link2ICT or Birmingham Audit. Screen captures may be covered by the Obscene Publications Act which prohibits transfer of such material.

As well as keeping a record of potential issues, ClassroomCloud generates an e-mail alert when a particular user generates a specific number of captures. For example:

- i) a pupil typing a number of pornographic terms trying to search for inappropriate information
- ii) a pupil receiving a number of messages containing threatening language

The settings for these alerts can be adjusted to suit the school environment and manage the amount of information that is generated and reported.

Following advice from the technical staff at the school, the senior leadership team must decide on the initial configuration of these alerts and then establish a process for managing and documenting any future configuration changes that are made to the system. All changes to the system should be signed off by the DSL/e-safety coordinator or Headteacher.

Staff information

ClassroomCloud is installed on WGPS computers. This includes staff laptops, and, as they are covered by the Acceptable Use policies both on and off the premises, the software is set to store and forward information on their use away from the network.

Staff are made aware that monitoring software is being used, what information may be captured and what processes are in place to protect their privacy. They are also reminded that our Acceptable Use Policies apply to all school equipment (including laptops) at all times, including when they are taken off site.

If there is a concern relating to a member of staff, advice must be taken from Birmingham Audit prior to any investigation being carried out. Staff data is considered private and must not be accessed without first establishing reasonable cause and completing the necessary City Council Documentation.

Limitations to accessing staff data

Monitoring overall staff usage ensures compliance with WGPS processes and Acceptable Usage Policies. However, any staff data recorded is considered private and access is limited to two named members of the Senior Leadership Team. In addition, archive or other stored data can only be accessed when there is a genuine cause for concern and advice must be sought from Birmingham Audit prior to carrying out any investigation. Unauthorised access or 'fishing' (i.e. just looking to see what people are doing) is not allowed and anything that is found in this way could not be used in any follow up action.

E-mail alerts from ClassroomCloud –

Pupil data: alerts will be sent to the DSL. The incident can then be followed up in line with our policies.

Staff data: Alerts will be sent to the Deputy Headteacher. In general, these alerts will be 'false positive' results generated as a result of staff carrying out their normal duties and will be helpful initially in configuring the software to exclude certain words or web sites from the monitoring. If the alerts raise a concern against a member of staff advice must be sought from Birmingham Audit before any investigation is carried out or any further log data is accessed.

E-mail alerts for staff should be set at a higher level than for pupils and time should be taken to exclude 'safe' web sites such as News and common 'false positive' words that may generate alerts. E-mail tools can then be used to filter these messages into a specific folder than can be periodically reviewed.

Technical staff will, as part of their role, have potential access to the staff data just as they have potential access to a range of private information on the school network, but they should be given clear guidance as to their role and understand that they should not access the data unless directed by the Headteacher.

Wylde Green Primary School

e-safety log - Incident Recording Form

Date	Time	Lesson / Room

Pupil	Form	Staff

Incident appears	Accidental	Malicious

Web site address:

Type of content:	CHAT	PORN	GAMES	GROSS
	OTHER: -			

Action Taken:

Reported? YES / NO	To:	

Further action required?

Staff Notice - When using I.T. equipment:

Start with Acceptable use and your rules

State what is allowed in the lesson

- if they are not using the Internet tell them, and the consequences

When using the Internet:

Provide web links, rather than letting pupils search

- this focuses the lesson and keeps them on task

Always test any search before the pupils

- plan the search with them and give appropriate key words

Always remind pupils about the risks and issues

- reinforce that accidental incidents are not an issue

Remember, if they are playing an unauthorised game in your lesson it is a behaviour issue that must be addressed.