Online Safety Policy

Overview

Online Safety encompasses Internet technologies 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.

Howley Grange's Online Safety policy will operate in conjunction with other policies including those for Computing, Acceptable Use, Behaviour, Bullying, Curriculum, Safeguarding and Data Protection.

Why Internet use is important?

The Internet is an essential element in 21st century life for education, business and social interaction. 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. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

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 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. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research on a range of devices, including personal computers, iPads and netbooks.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, receiving regular information about Online Safety incidents and monitoring reports.

Head Teacher and Senior Leaders:

The Head Teacher is responsible for ensuring the safety (including Online Safety) of members of the school community. The day to day responsibility for Online Safety will be delegated to the DSL / Online Safety

Co-ordinator.

- The Head Teacher / SLT are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use Computing tools such as the Internet, email and social networking sites, safely and appropriately.
- The Head Teacher / SLT 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 SLT will receive regular monitoring reports from the Online Safety Co-ordinator.
- The Head Teacher and DSL (Designated Safeguarding Lead) 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 Head Teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this online facility.

Designated Safeguarding Lead (DSL) / Online Safety Co-ordinator (K Trueman-Brown)

The named person is trained in Online Safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Their responsibilities include:

- Liaising with the Local Authority
- Receiving reports of Online Safety incidents and creating a log of incidents to inform future Online Safety developments.
- Attending relevant meetings / Governor Committee meetings.
- Taking day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing the school Online Safety policies and documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Providing training and advice for staff.
- Liaising with school Computing technical staff and school contact from the managed service provider- SIPS.

Managed service provider

The managed service provider is responsible for helping the school to ensure that it meets the Online Safety technical requirements outlined by LGfL. The managed service provides a number of tools to schools including Smart cache servers, Smooth wall and ESafe Monitoring Solution, which are designed to help schools keep users safe when online in school. Schools are able to configure many of these locally or can choose to keep standard settings. The LGfL Client team work with school representatives to develop and update a range of Acceptable Use Policies and any relevant Local Authority Online Safety policy and guidance. Members of the LGfL team will support schools to improve their Online Safety strategy. The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact SIPs

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 encourage pupils to develop good habits when using Computing to keep themselves safe.
- They have read, understood and signed the school Staff Acceptable Use Policy (appendix 4).
- They report any suspected misuse or problem to the Online Safety Co-ordinator, Head Teacher, Deputy Head or Assistant Head for investigation.
- Digital communications with pupils (email / Virtual Learning Environment) 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 school activities.
- Pupils understand and follow the school Online Safety and Pupil Acceptable Use Policy (appendix 3a and 3b)
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor Computing activity in lessons, extra-curricular and extended school activities.
- They are aware of Online Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school 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. They include the teaching of Online Safety in their lessons.

Pupils

Pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure and safe system provided through SIPS.

Pupils:

- Are responsible for using the school Computer systems within the safety limits set by staff.
- Need to 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites and on cyber-bullying.
- Will 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 the use of an externally available web-based system, provided by the school. During school time children will be trained on acceptable use of Microsoft Teams and will be instructed on how to use it safely.

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, the school website and information about national or local Online Safety campaigns or literature. Parents and carers will be responsible for:

- Accessing the school website, in accordance with the relevant school Acceptable Use Policy.
- Promoting an appropriate and safe use of the Internet with their children.

Policy Statement

Education – pupils

There is a planned and progressive Online Safety curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.

Online Safety education is provided in the following ways:

- A planned Online Safety programme is provided as part of the Computing and PSHE curriculum and is regularly revisited – this includes the use of ICT and new technologies in school and outside school.
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils are taught in all lessons to be aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of Computer systems and the Internet are posted around school.
- Pupils are taught the importance of information security and the need to keep information such as their password safe and secure.
- Staff act as good role models in their use of Computing, the internet and mobile devices.
- All pupils read, understand and accept the Pupil Acceptable Use Policy.

Education – parents / carers / wider community

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world. The school provides information and awareness to parents and carers through:

- Letters
- The designated area of the school website for 'Online Safety.'
- Parents' evenings

Education & Training – Staff

All staff receive annual Online Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal Online Safety training is made available to staff.
- All new staff receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy.
- The Online Safety Co-ordinator / DSL receives regular updates through attendance at YourIG, LA and other information or training sessions and by reviewing guidance documents released by DfE, LA, YourIG and others.
- This Online Safety policy and its updates are presented to and discussed by staff in staff meetings.
- The Online Safety Co-ordinator provides advice, guidance and training as required to individuals.

All staff are familiar with the school Online Safety, Computing and Acceptable Use Policy regarding:

- Safe use of e-mail.
- Safe use of the Internet including use of Internet-based communication services, such as instant messaging and social network.
- Safe use of the school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.

- Publication of pupil information/photographs and use of the school website.
- Cyberbullying procedures.
- Their role in providing Online Safety education for pupils.
- The need to keep personal information secure.

Training – Governors

Governors take part in Online Safety awareness sessions, particularly those who are members of any sub-committee / group involved in Computing or Online Safety, Health and Safety or Safeguarding.

This is offered by:

- Attendance at training provided by the Local Authority.
- Participation in school training or information sessions for staff.

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

- The school Computer systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the Acceptable Use Policies.
- There will be regular reviews and audits of the safety and security of school Computer systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school Computer systems.
- All users will be provided with a username and password.
- The school maintains and supports the managed filtering service provided by SIPS.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school can provide enhanced user-level filtering through the use of the Smart Cache/Safety Net Universal.
- The school manages and updates filtering issues through the SIPS helpdesk.
- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Co-Ordinator and Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Governor.
- An appropriate system is in place for users to report any actual or potential Online Safety incident to the relevant person.
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access to “guests” (e.g. trainee teachers, visitors) onto the school system.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices as stated in the Acceptable Use Policies.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online Safety is a focus in all areas of the curriculum and staff reinforce Online Safety messages in the use of Computing across the curriculum.

- In lessons, where the Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the pupils visit.
- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- 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 Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged.
- Pupils are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet. Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Child Line or CEOP report abuse button.

Mobile Technologies

Mobile technology devices may be school owned / provided by the LA in response to the need for remote education due to COVID-19 restrictions. They usually have the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile device in a school context is educational, even if they are permitted to take them home. If the device is to be taken home a 'Guardianship Form' will be completed and signed for.

Use of digital and video images

When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the sharing, distribution and publication of those images as stated in the Acceptable Use Policies. Those images are only taken on school equipment; the personal equipment of staff are not used for such purposes.
- Care is taken when capturing digital or video images, ensuring pupils are appropriately dressed and that they 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 comply with the school 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.
- Written permission from parents or carers is obtained before photographs or images of pupils are published on the school website.

- Pupil’s work can only be published with the permission of the pupil and parents or carers. Parents should have signed the DSCB consent form.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school will ensure that:

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

Staff must ensure that they:

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

Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems e.g. by remote access from home.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the DSL, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and parents / carers (email) or with pupils (Microsoft Teams) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Mobile phones may be brought into school by students when they are arriving or leaving school unaccompanied by an adult in Years 5 and 6 ONLY. They must be handed in at the start of the day and kept securely in the school office. A consent form must have been prior obtained from a parent / guardian.
- The school allows staff to bring in personal mobile phones and devices for their own use. Mobile phones should not be used in the presence of pupils as outlined in the Acceptable Use Policies. Under no circumstances should a member of staff contact a pupil or parent / carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Unsuitable / inappropriate activities

The school will take all reasonable precautions to ensure Online Safety is a key focus. Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about unacceptable use and possible sanctions. Sanctions available include:

- Interview by Class Teacher, Online Safety Co-ordinator or Head Teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period.
- Referral to LA / Police.

The DSL acts as first point of contact for any issues regarding safeguarding and these will be dealt with in accordance with our school and LA Safeguarding procedures. Any complaint about staff misuse is referred directly to the Head Teacher. The Online Safety Co-ordinator / DSL is responsible for all other complaints and issues. Instances of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. There are however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. If any such cases arise, each will be dealt with appropriately under the relevant policies and guidance.

Date: November 2022

Date for review: November 2024

K Trueman-Brown

This Online Safety Guidance and Policy has been written with references to the following sources of information:

BECTA

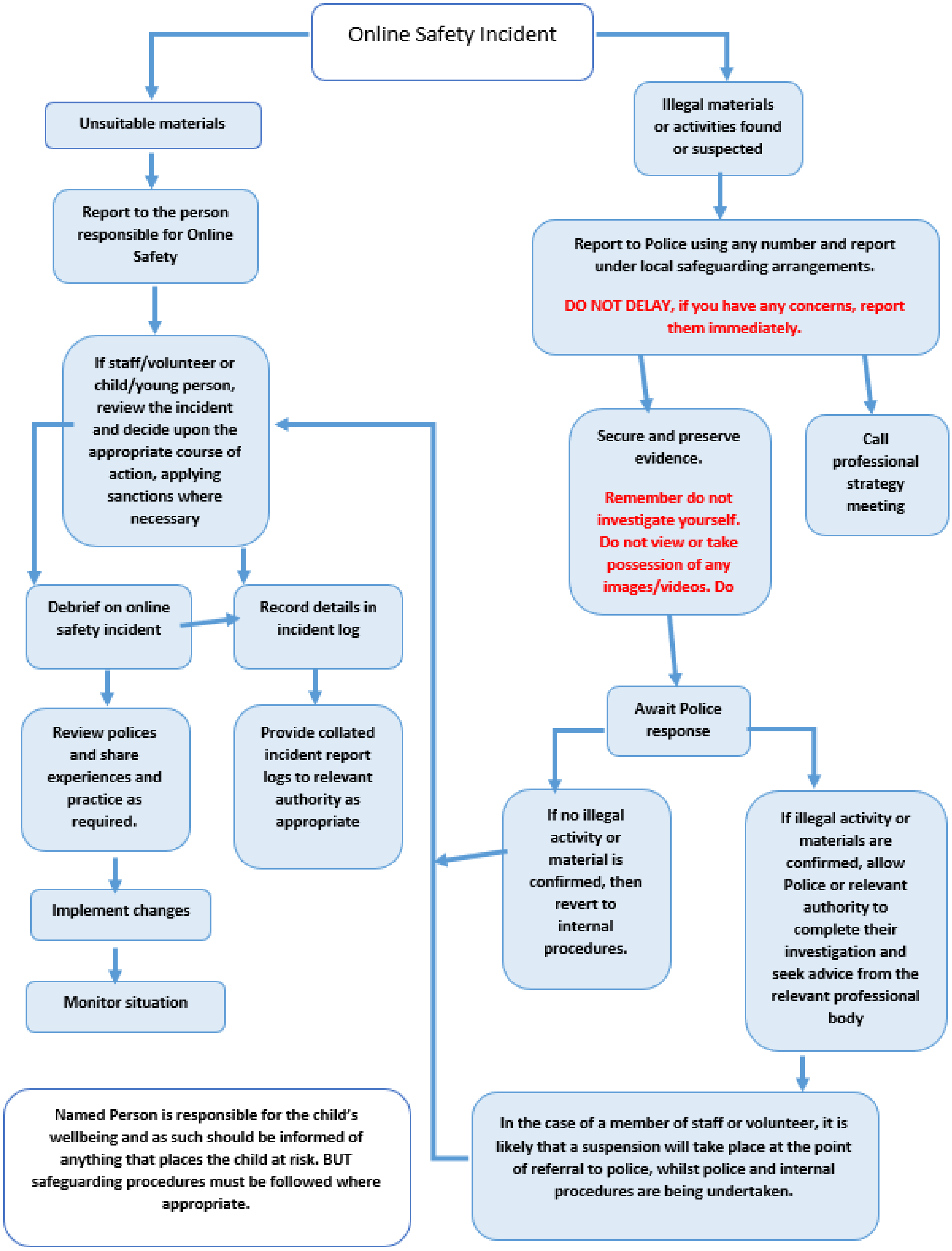
Dudley LA

Keeping Children Safe in Education 2023

Appendix 1 - Additional information and guidance

Dudley- Safe and Sound	https://www.dudleysafeandsound.org/onlinesafety
Online Harms White Paper	https://www.gov.uk/government/consultations/online-harms-white-paper
DfE- Preventing and Tackling Bullying (2017)	https://www.gov.uk/government/publications/preventing-and-tackling-bullying
Keeping Children Safe in Education	https://www.gov.uk/government/publications/keepingchildren-safe-in-education--2
Working Together to Safeguard Children	https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
Safeguarding and Child Protection Policy	https://safeguarding.dudley.gov.uk/safeguarding/child/
Searching, Screening and Confiscation at School	https://www.gov.uk/government/publications/searching-screening-and-confiscation
Revised Prevent Duty	https://www.gov.uk/government/publications/prevent-duty-guidance

Appendix 2 - Online safety sample response flowchart (Provided by SWGfL Online Safety School)



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

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.

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.

Appendix 3a – Key Stage 1 Acceptable Use Policy

Howley Grange Primary School

Pupil Acceptable Use Policy (KS1)

We have many computers and devices at school to help our learning. These rules will keep everyone safe and help us to be considerate to others. It is important that I read this policy (or listen to it being read to me) carefully. If there is anything that I do not understand, I will ask my teacher.

I agree that:

I will only use my own username and password to log on. I will not share my password with anyone.

I will use the technology at school for learning and use the internet and equipment properly.

I will only use websites and software that have been suggested by my teacher or a grown up.

If anyone sends me a message or image I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will not tell anyone my name, where I live or where I go to school without permission from my teacher or my parent.

I will tell a grown up if I feel scared or unhappy about anything that I find on the school computers, laptops, cameras, or ipads.

I know anything I do on the computer may be seen by someone else.

Signed :………

PRINT NAME :……

Dated : ……………………………………………………………….

Appendix 3b – Key Stage 2 Acceptable Use Policy

Howley Grange Primary School

Pupil Acceptable Use Policy (KS2)

The school has installed computers, supplied a range of devices and provided Internet access to help our learning. These rules will keep everyone safe and help us to be considerate to others. It is important that I read this policy carefully. If there is anything that I do not understand, I will ask my teacher.

I understand that the school may check my computer files, may monitor any Internet sites I visit and may read any communication I have with others using the school network.

I agree that:

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write inappropriate comments or participate in online bullying. If anyone sends me images or messages I do not like or feel uncomfortable about, I will save it and show it to my teacher or parent. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes, games or apps on to the school computers, laptops or ipads unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio, photographic or video recordings of another pupil, teacher or adult without their permission.

When using sites on the internet, I will not give mine or anyone else's name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. I know content on the web is someone's property and I will ask a responsible adult if I want to use information, pictures, video, music or sound to ensure I do not break copyright law.
I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information - text, images or sounds - and say it is my own work).

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

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

If I bring a mobile phone to school (in accordance with the mobile devices policy) I must turn it off and hand it in at the start of the day, and it will be returned to me at the end of the day. I will always think carefully about how I send or reply to messages, comments and images.

Signed :……

PRINT NAME :………

Dated : ………………………………………………………………

Appendix 4 – Staff Acceptable Use Policy

Howley Grange Primary School

Staff Acceptable Use Policy

Rules for Responsible Internet use

This policy applies to all adult users of the schools systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or another member of the Senior Leadership Team. Once you have read and understood this policy thoroughly, you should sign to say that you have read and understood it and retain a copy for your own records.

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

SIPS has a contractual obligation to monitor the use of the internet and e-mail services provided as part of LGFL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically. GDPR regulations and guidelines should be considered when using personal data.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of SLT immediately.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

- You should not:
  - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
  - seek to gain access to restricted areas of the network;
  - knowingly seek to access data which you are not authorised to view;
  - introduce any form of computer viruses;
  - carry out other hacking activities.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.
Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is inevitable in today's society. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter

When using social networking sites the following statements apply:-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @howley.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school.
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm.
- The school social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the Data Protection Act 1998 and 2018. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work, personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must:-

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 2018 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

PRINT NAME: …………………………………………. Signed:………………………………………

Date: …………………..