Online Safety Policy

Policy updated: November 2022

Policy to be reviewed: **November 2024**

Schedule for Development / Monitoring / Review

The implementation of this Online Policy will be monitored by: Maria Hughes Business Manager/DSL and Emma Collins Online Coordinator
Should serious online incidents take place, the following external persons / agencies should be informed: LA, ICT Manager, LADO, Police and any other relevant agency working with the child and family.

The school will monitor the impact of the policy using:
• Logs of reported incidents;
• Monitoring logs of internet activity (including sites visited);
• Internal monitoring data for network activity;
• Surveys / questionnaires of pupils, parents / carers and staff.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying Policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place in and out of school.

Roles and Responsibilities

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

Management Committee

The Management Committee are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Management Committee receiving regular information about online incidents and monitoring reports. The Management Committee will receive a report on the implementation of the Online Policy generated by the monitoring group (which will include anonymous details of online incidents) at regular intervals. The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online or incidents that have taken place.

Senior Leadership Team

- The Headteacher has a duty of care for ensuring the safety (including online) of members of the school community, though the day to day responsibility for online will be delegated to the Online Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (see appendix flow chart on dealing with online incidents – Responding to incidents of misuse and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Senior Leadership Team are responsible for ensuring that the Online Coordinator and other relevant staff receive suitable training to enable them to carry out their online roles and to train other colleagues, as relevant.
- The Senior Leadership Team 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 monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Co-ordinator.

Online Coordinator

- Leads the Online Working Party.
- Takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school Online Policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff.
- Receives reports of online incidents and creates a log of incidents to inform future online developments.
- Meets regularly with DSL / Senior Leadership Team to discuss current issues, review incident logs and filtering / change control logs.
- Attends Management Committee meetings when appropriate.

Network Manager

The Network Manager, in conjunction with the IT supplier, is responsible for ensuring:

- The schools technical infrastructure is secure and is not open to misuse or malicious attack;
- The school meets required online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply;
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- They keep up to date with online technical information in order to effectively carry out their online role and to inform and update others as relevant;
- The use of the network / internet / virtual learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online Coordinator for investigation / action / sanction;
- Monitoring software / systems are implemented and updated.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online matters and of the current school Online Policy and practices;
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA);
- They report any suspected misuse or problem to the Senior Leadership Team for investigation / action / sanction;

- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems;
- Online issues are embedded in all aspects of the curriculum and other activities;
- Pupils understand and follow the online and acceptable use policies;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor the use of digital technologies, mobile devices, cameras etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- That LAN School is used effectively to monitor and control internet use in lessons.

Designated Safeguarding Lead

Should be trained in online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

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

- Digital and video images taken at school events;
- Access to parents' sections of the website / VLE and on-line pupil records;
- Their children's personal devices in the school (where this is allowed).

Policy Statements

Education – Pupils

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

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

- A planned online curriculum should be provided as part of Computing / PHSE / SPICE Time / other lessons and should be regularly revisited;
- Key online messages should be reinforced as part of a planned programme of small group activities / 1 : 1;
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

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

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

- Curriculum activities;
- Letters, newsletters, web site, VLE;
- Progress Review Meetings;
- High profile events / campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online;
- The school website will provide online information for families and the wider community.

Education & Training – Staff / Volunteers

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

- A planned programme of formal online training will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly;
- All new staff should receive online training as part of their induction programme, ensuring that they fully understand the school Online Policy and Acceptable Use Agreements;

- The Online Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations;
- This Online Policy and its updates will be presented to staff to be read and understood. It will be covered and discussed in staff online training;
- The Online Coordinator will provide advice, guidance and training to individuals as required.

Training – Management Committee

Management Committee should take part in Online Training / Awareness Sessions.

- By participation in school training and information sessions for staff or parents.

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school has a Service Level Agreement with an external IT provider (Medhurst) who jointly are responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their t-safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password (by either Jamie Southwell – Medhurst, or Emma Collins – Online Coordinator). The IT Manager will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place (e.g. school safe).
- The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Filtering is controlled by HCC's HPSN service. The school have access to the Flexible Web Filtering portal, and are able to make changes for categories or individual websites. The school is not able to override certain categories which are deemed to be inappropriate for schools. The content of the lists of URLs in the categories are constantly updated, this is part of the BlueCoat solution that HPSN uses. Staff send an email to the IT Technician, who then logs a ticket on the helpdesk and makes the change. If the request is unusual the IT Technician will ask the Headteacher to approve.
- The procedure for filtering change requests:
    - Staff member logs a ticket (emails support@medhurst-it.com);
    - The IT Technican gets authorisation from the Business Manager or Headteacher;
    - The Change is implemented;
    - The Change is recorded on the spreadsheet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc.).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might

threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed ICT policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Staff are to use Anycomms in such instances.

Use of Digital and Video Images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- When the school holds events involving parents e.g. sports day, to respect everyone's privacy and in some cases protection, parents will have requested not to take images of pupils.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and ensure that parents / carers have given written permission.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

General Data Protection Regulation (GDPR)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold 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;
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing";

- It has a Data Protection Policy It is registered as a Data Controller for the purposes of the General Data Protection Act (GDPA);
- Responsible persons are appointed / identified - General Data Protection Officer (GDPO);
- Risk assessments are carried out to assess how data is shared, stored and processed;
- It has clear and understood arrangements for the security, storage and transfer of personal data;
- Data subjects have rights of access and there are clear procedures for this to be obtained;
- There are clear and understood policies and routines for the deletion and disposal of data;
- There is a policy for reporting, logging, managing and recovering from information risk incidents;
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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;
- Use personal data 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;
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected;
- the device must be password protected;
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

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

- The official school email service may be regarded as safe and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (by remote access);
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- Any digital communication between staff and pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official, monitored school systems. Personal email addresses, text messaging or social media must not be used for these communications;
- Whole class and group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use;
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

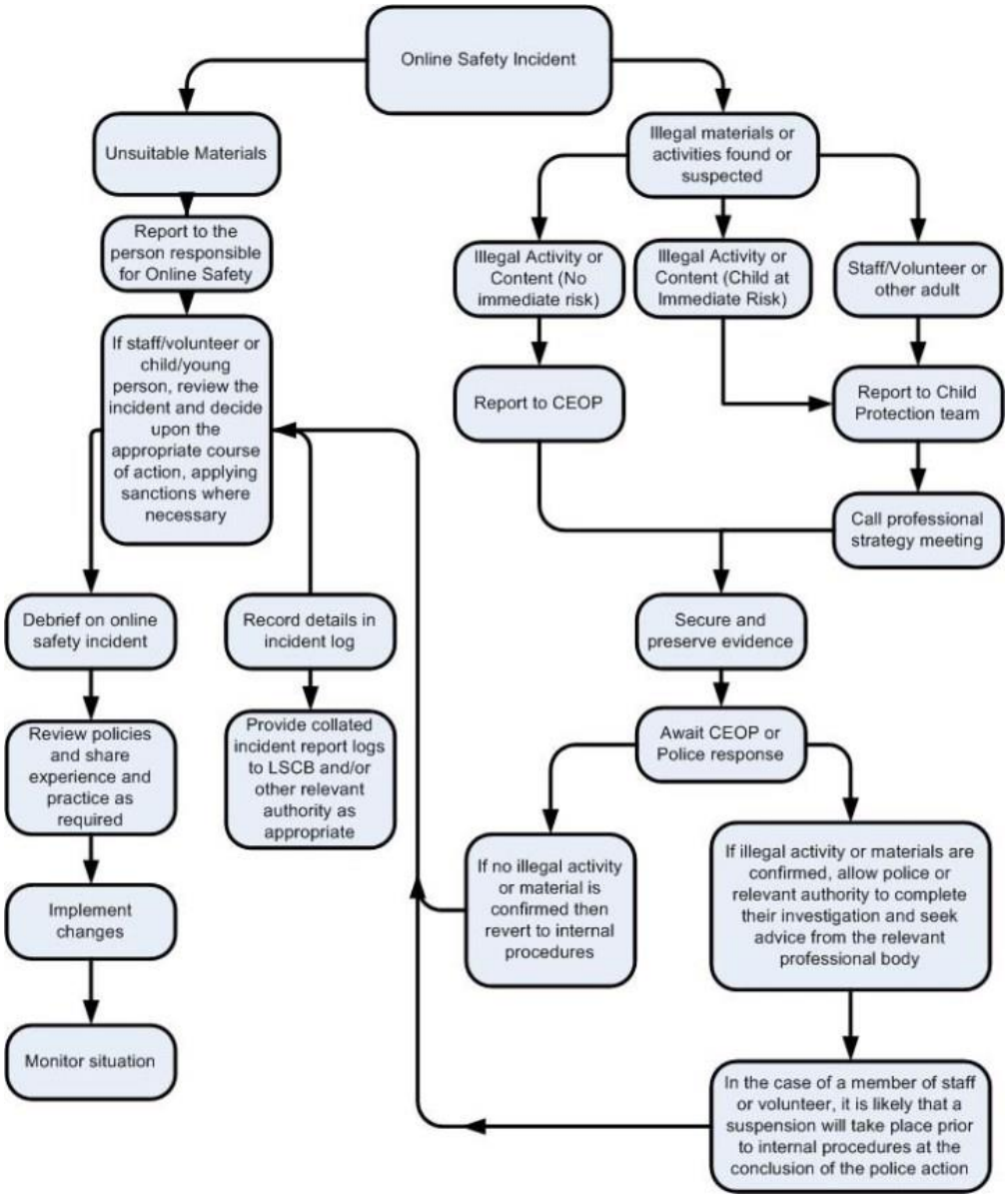
Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

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

Appendix 1: **Flowchart for dealing with Online Incidents**



Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures;
    - Involvement by Local Authority or national / local organisation (as relevant);
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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