HALESBURY SCHOOL

E SAFETY POLICY

Policy for the attention of			
Audience	Key Audience	Optional Audience	Additional/Notes
Senior Leadership Team	✓		
Teachers	✓		
Teaching Assistants	✓		
Administrative Staff	✓		
Curriculum support	✓		
Lunchtime Supervisors	✓		
Site Manager	✓		
Cleaners	✓		
Governors	✓		
Parents	✓		
Website	✓		
Local Authority	✓		

Responsibility of	Head Teacher
Review frequency	Annually
This version agreed	18/10/2018
Next review date	October 2020

Halesbury School Policy For E-Safety (Online Safety) Guidance

This policy also incorporates:

- *Mobile Technology Policy (inc. BYOD Policy)*
- *Social Media Policy*

Table of Contents

Scope 5
Development, Monitoring and Review of the E-Safety Policy 5
Roles and Responsibilities 6
Governors 6
Head teacher and Senior Leaders 6
E-Safety Coordinator / Officer 7
Managed service provider (applicable to DGfL3 schools) 7
Teaching and Support Staff 8
Designated person for Child Protection / Child Protection Officer 9
E-Safety Committee 9
Students / pupils: 9
Parents / Carers: 10
Community Users/ 'Guest Access' 10
Online Safety Committee Terms of Reference 11
Policy Statement 12
Education – students / pupils 12
Education – parents / carers 13
Education - Extended Schools 13
Education & Training – Staff 13
Training – Governors 14
Technical – infrastructure / equipment, filtering and monitoring 14
Curriculum 16
Use of digital and video images 17
Data Protection 17
Communications 18
Unsuitable / inappropriate activities 19
Mobile Technology Policy (inc. BYOD Policy) 20
Safe use of mobile technology 20

When personal devices are permitted..... 21
Social Media Policy 22
Scope 22
Organisational Control 23
Roles & Responsibilities 23
SLT 23
Administrator / Moderator 23
Staff 24
Managing accounts 24
Monitoring 24
Behaviour 24
Legal considerations 25
Handling abuse 25
Tone 26
Use of images 26
Personal use 26
Monitoring posts about the school 27
Appendices 28
Appendix 1 - Guidance reporting for E-Safety incidents 28
Appendix 2 - E-Safety tools available on the DGfL network 29

Scope

This guidance applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy should be reviewed in line with the School Information Security Policy.

Development, Monitoring and Review of the E-Safety Policy:

This E-Safety policy has been developed by a committee made up of:

- Head teacher / Senior Leaders
- ICT Technical staff
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School / Student / Council
- INSET Days
- Governors meetings / sub-committee meetings
- Parents evening
- School website / newsletters
- The results of surveys/questionnaires with specific reference to e-safety

The school will monitor the impact of the policy using:

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys / questionnaires of stakeholders-including ‘pupil voice’

The make-up of the E-Safety committee is outlined in the ‘Online Safety Committee Terms of Reference’ See below.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Committees, receiving regular information about E-Safety incidents and monitoring reports- (It is suggested that Governing Bodies review their E-Safety Policy at the start of each academic year to ensure that all new staff and pupils are aware of its content and have signed appropriate Acceptable Use Policies).

A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinator / Officer (ESO)
- Regular updates on the monitoring of E-Safety incident logs
- Regular updates on the monitoring of the filtering of web sites
- Reporting to relevant Governor meetings

Head teacher and Senior Leaders:

The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO). The schools SIRO is responsible for reporting security incidents as outlined in the schools

Information Security Policy. The day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator / Senior Management Team (SLT) who has this responsibility

- The SLT are responsible for ensuring that the E-Safety Coordinator receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately.
- The 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 E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles-

(DGfL has produced guidance relating to the reporting procedure for E Safety incidents- see appendix 1. This should be viewed in conjunction with the Child Protection reporting procedures, in connection to the nature of the incident)

- The SLT will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Head teacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff- (DGfL has produced guidance relating to the reporting procedure for E Safety incidents- see appendix 1. This should be

viewed in conjunction with Child Protection reporting procedures, in connection to the nature of the incident)

- The Head teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via an online communication system, have adequate information and guidance relating to the safe and appropriate use of this on line facility- (The Information Security Policy contains detailed guidance).
- The Head teacher or a designated member of the SLT is responsible for ensuring that parents/carers understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures. Safeguarding procedures are outlined in the child protection policy.
- Taking day to day responsibility for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies / documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority, DO (LADO) or relevant organisations.
- Liaising with the schools SIRO to ensure all school data and information is kept safe and secure.
- Liaising with school ICT technical staff.
- Receiving reports of E-Safety incidents and creating a log of incidents to inform future E-Safety developments.
- Attending relevant meetings.
- Reporting regularly to the Senior Leadership Team

Managed service provider (applicable to DGfL3 schools):

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by DGfL. The managed service provides a number of tools to schools including Securus (optional), Smoothwall filtering and MDMs (Mobile Device Management systems), which are designed to help schools keep users safe (see appendix 2).

Schools are able to configure many of these locally or can choose to keep standard settings.

A designated adult can access activity logs for network users and apply 'rules' to specific group of users. Schools/settings should nominate a suitable member of staff to manage this responsibility.

CC4 Anywhere is a facility that enables a user to access documents and applications stored on the school server/servers. The school has responsibility for ensuring files and applications accessed via this system comply with information and data security practices. Schools/settings may wish to specify the type of information that users can access via CC4 Anywhere.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Policies/guidance and include relevant Local Authority E-Safety policies and guidance.

Members of the DGfL team will support schools to improve their E-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 the DGfL team.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E- Safety policy and practices
- They encourage pupils to develop good habits when using ICT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP/AUA)
- They report any suspected misuse or problem to the E-Safety Co-ordinator /Senior Leader for investigation
- Digital communications with students / pupils (email / Virtual Learning Environment (VLE) applications/O365 Apps/Google Apps / voice) should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- Students / pupils understand and follow the school E-Safety and acceptable use policy
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices, including their personally owned devices and that they monitor their use and implement current school policies with regard to the use of these devices in school or during extended school activities. A guardianship/loan form is available for schools to adapt for school owned equipment used by staff.
- In lessons, where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. They include the teaching of E-Safety in their lessons
- Pupils understand that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with the AUP/AUA or any statements included in other policies- E.G: Behaviour Policy

- Pupils understand that the school may investigate any reported misuse of systems, by pupils, out of school hours as part of 'safeguarding' procedures

Designated person for Safeguarding:

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

- Sharing of personal data
- Publishing of specific information relating to school based activities involving pupils, via official school systems such as the school web site, Twitter, Facebook, You Tube
- Sharing of school owned devices or personal devices that may be used both within and outside of school
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying, Sexting and Sextortion, Revenge porn, Radicalisation

Students/Pupils:

Students/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, monitored and safe system provided through DGFL. Students/pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy/AUA which they will be expected to sign before being given access to school systems
- 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, video streaming facilities, digital image sharing sites and cyber-bullying
- Are responsible for the safe use of school owned equipment at home, in accordance with the school AUP/AUA, for these devices.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to the use of an externally available web based system, provided by the school
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, may be investigated by 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 therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about E-Safety campaigns Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Accessing the school website / School Learning Platform/ on-line student / pupil records or other school provided system (specify here) in accordance with the relevant school Acceptable Use Policy/AUA.

Community Users/ 'Guest Access':

Community Users who access school ICT systems / website / School Learning Platform/on- line student/pupil records or other school provided system (specify here) as part of the Extended School provision will be expected to sign a Community User AUP/AUA before being provided with access to school systems.

Guest wireless access is available at Halesbury School to users of the network who do not have a permanent username and password to access the Halesbury Network. Guest wireless access will be given to authorised users on request.
The level of access will be determined against the role of the user in line with our filtering policy.
Guest users will be made aware of the policies and procedures that apply to online safety. Guest users will read, understand and sign a guest user AUA before username and password details are disclosed.

Online Safety Committee Terms of Reference:

Purpose

To provide a consultative group that has wide representation from the [school/ academy] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

Membership

2.1 The online safety committee will seek to include representation from all stakeholders. The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Student representation

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

Duration of Meetings

Meetings shall be held when appropriate for a designated period of time. A special or extraordinary meeting may be called when and if deemed necessary.

Functions

These are to assist the online safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites)
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

Policy Statement

Education – students / pupils

There is a planned and progressive E-Safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. E-Safety education is provided in the following ways:

- A planned E-Safety/E-literacy programme is provided as part of ICT / PHSE / and is regularly revisited – this include the use of ICT and new technologies in school and outside school
- Key E-Safety messages are reinforced as part of a planned programme of assemblies and tutorial activities

- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy and plausibility of information
- Students / pupils are aware of the Student / Pupil AUP (AUA) and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / 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 ICT systems / internet are posted in all rooms and are specified in separate policies relating to the use of school endorsed systems
- Students and 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 ICT, the internet and mobile devices

Education – parents / carers

The school provides information and awareness to parents and carers through

- Letters, newsletters, School web site
- Parents evenings
- E-Safety sessions for parents/carers
- Family learning opportunities

Education - Extended Schools

The school offers family learning courses in ICT, digital literacy and E-Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around E- Safety are targeted towards grandparents and other relatives as well as parents. 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.

Education & Training – Staff

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

- A planned programme of formal E-Safety training is made available to staff. An audit of the E-Safety training needs of all staff is carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process
- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies

- The E-Safety Coordinator (or other nominated person) receives regular updates through attendance at DGfL / LA / training sessions and by reviewing guidance documents released by DfE / DGfL / LA, LSGB and others.

- This E-Safety policy and its updates are presented to and discussed by staff in staff meetings / INSET days
- The E-Safety Coordinator provides advice / guidance / training as required to individuals

All staff are familiar with the schools' Policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other school approved system
- Safe use of school network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs/videos/posts/blogs and information available on the school website
- Capturing and storing photographs/videos/audio files on personal and school owned devices
- Cyberbullying procedures
- Their role in providing E-Safety education for pupils
- The need to keep personal information secure

Staff are reminded / updated about E-Safety matters at least once a year.

Training – Governors

Governors take part in E-Safety training sessions, particularly those who are members of any sub-committee / group involved in ICT / E-Safety / Health and Safety / Child Protection.

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL/ LSGB or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school is monitored by a piece of Software called Forensic Monitor. Information on monitored inappropriate content or language is sent to the Head teacher and ICT Technician. This information can only be accessed via a password held by the Head teacher and the ICT Technician.

The managed service provider is responsible for ensuring that the school 'managed' infrastructure / network is as safe and secure as is reasonably possible.

The school is responsible for ensuring that policies and procedures approved within this document are implemented.

School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies/AUA's

There will be regular reviews and audits of the safety and security of school ICT systems

- Servers, wireless systems and cabling must be securely located and physical access restricted to authorised users

All users will have clearly defined access rights to school ICT systems

- All users Students/ Staff will be provided with a username and password
- Users will be required to change their password every 30 days minimum
- Generic passwords are issued for Class Based SEN pupils. Staff are made aware of the risks associated, and the rules set out in the policy and the AUP/AUA)
- 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 maintains and supports the managed filtering service provided by DGfL The school can provide enhanced user-level filtering through the use of Smoothwall filtering or a MDMs (Managed Mobile Device system)
- The school manages and updates filtering issues through the ICT Technical Staff / RM Service desk
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential E-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 downloading of executable files by users – Restrictions prevent executable files from working without permissions given by RM Service Team
- 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 – Students are not to use memory sticks and Staff are not

to place sensitive documentation onto any removable media without authorisation from SLT

- 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
- The school has responsibility for ensuring files and applications accessed via CC4 Anywhere comply with information and data security practices. Information that users can access via CC4 Anywhere is governed by the school.

Curriculum

E-Safety is a focus in all areas of the curriculum. The new Computer Science Curriculum specifically identifies 'Digital Literacy' as a focus. Digital Literacy should be taught. Staff will reinforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students / 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 students / pupils are allowed to freely search the internet, eg using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- The school teaches 'Digital Literacy' as part of the new 'Computer Science' programme of study.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and 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
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students / pupils 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, Sexting and Sextortion, Revenge Porn and Radicalisation and know how to seek help if they are affected by any form of online bullying or exploitation. 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 Childline or CEOP report abuse button

Use of digital and video images

When using digital images, staff inform and educate students / 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 storing sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils are NOT permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the pupil's device.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and comply with good practice guidance on the use of such images
- Students' / 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 of students / pupils are published on the school website
- Student's / pupil's work can only be published with the permission of the student / pupil and parents or carers. Parents should have signed the DSCB consent form

Data Protection

Personal data will is 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.

Staff are aware of the 'School Information Security Policy'. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices , at school and home, or school systems 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, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot 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 once it has been transferred or its use is complete.

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 and students / pupils 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- (If staff use none standard or personal email accounts these are not secure and cannot always be monitored)
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, 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 students / pupils or parents / carers (email, chat, school VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Students / pupils are provided with individual school email addresses for educational use

- Students / 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 not be brought into school by pupils/students
- The school allows staff to bring in personal mobile phones and devices for their own use. 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 member 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
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via a Learning Platform or similar system. Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites.

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety is a key focus. 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 infringements in use and possible sanctions.

Sanctions available include:

- Interview/counselling by tutor / E-Safety Coordinator / Head teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to LA /DO (LADO)/ Police.

The LA has set out the reporting procedure for E-Safety incidents (see Appendix 1).

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school / LSGB child protection procedures.

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.

Mobile Technology Policy (inc. BYOD Policy)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils, staff and the wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices

Safe use of mobile technology:

- All school devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)

- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link

between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.

- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

When personal devices are permitted

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass- codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- Overnight excursions and trips – during an overnight excursion or trip it is expected that all mobile devices will be only be allowed with authorisation from the Senior Management. The same protocols, procedures and expectations, as outlined in this policy, apply for students while on a residential, which will be left to the discretion of the teacher in charge.

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

- Devices may not be used in tests or exams
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses

- School devices are provided to support learning.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Pupils must hand in their mobile devices to the school office at the start of the day to be locked away for safety.

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example; Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered.

Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational Control

Roles & Responsibilities

SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

Administrator / Moderator

- Create the account following SLT approval

- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- **Process for creating new accounts**

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate

training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

- Digital communications by staff must be professional and respectful at all times and in accordance with this policy.
- Staff will not use social media to infringe on the rights and privacy of others or make ill- considered comments or judgments about staff.
- School social media accounts must not be used for personal gain.
- Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

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

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy and GDPR Guidelines. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

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

Pupil/Students

- Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.

- The school's education programme should enable the pupils/students to be safe and responsible users of social media.
- Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

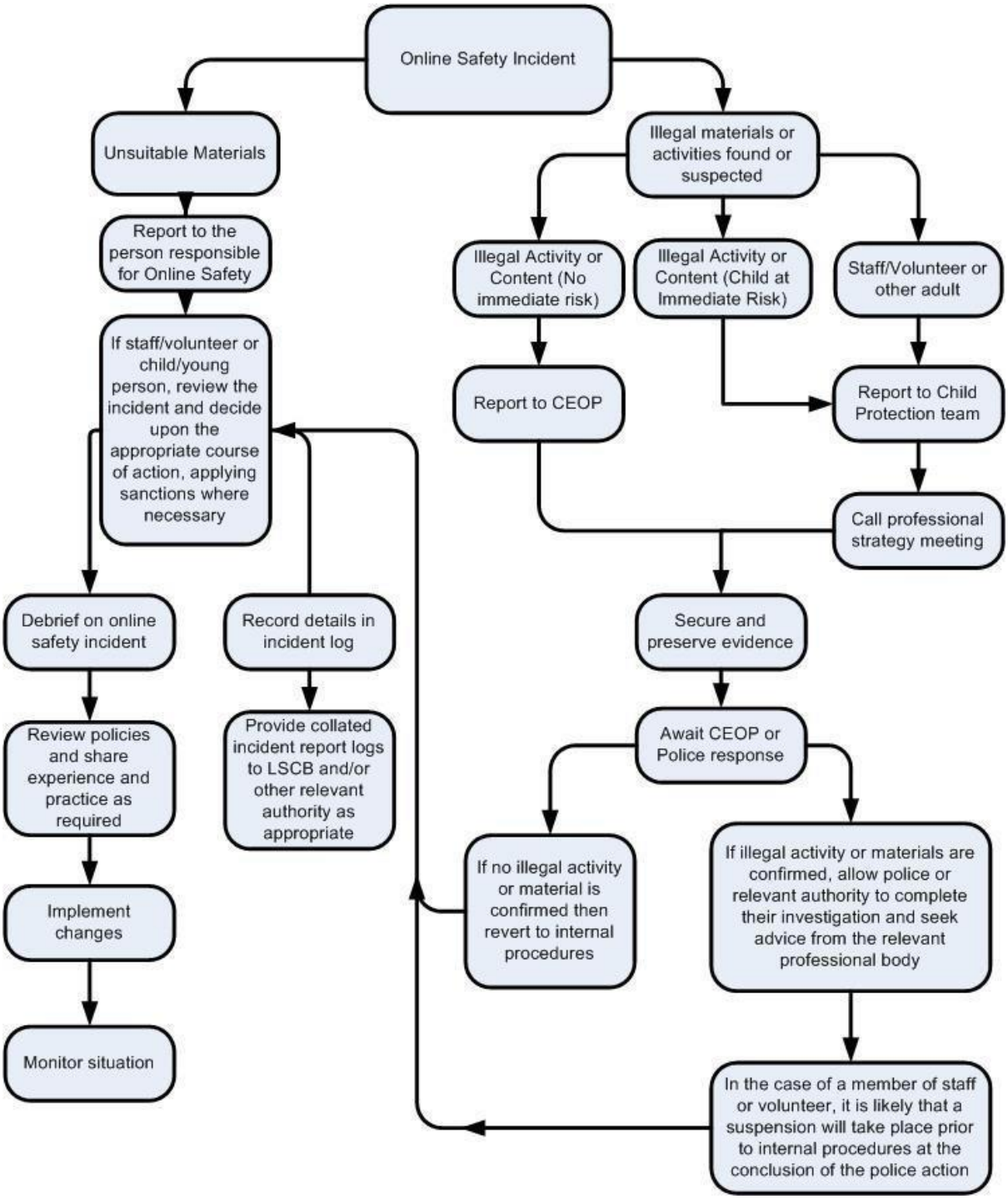
- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendices

Appendix 1 - Guidance reporting for E-Safety incidents



Appendix 2 - E-Safety tools available on the DGfL network

E-Safety tool	Type	Availability	Where	Details
Smoothwall filtering	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUP/AUA	Awareness raising	Part of CC4- needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
Securus (optional implementation)	Monitoring software- *licenses available on Linux and Apple devices*	Available to all schools who sign an agreement and attend training	All school Windows 7 or 8.1 managed desktops and managed networked laptops	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored
Email	Filtering and list control	Provided as part of DGfL	Office 365	Allows schools to restrict where email is sent from/to
RM Password Plus	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management tool that enforces password rules of complexity and length for different users