Finding Pathways to Learning & Living

Derrymount School

Online Safety Policy

November 2023

Development / Monitoring / Review of this Policy Schedule for Development / Monitoring / Review

The online safety policy was approved by the governing body on:	16th November 2023
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator
The Online Safety Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Cathy Clay
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, MASH, Police

The school will monitor the impact of the policy using:

• Logs of reported incidents

• Monitoring logs of internet activity (including sites visited) / filtering

• Internal monitoring data for network activity

• Surveys / questionnaires of:

Pupils / parents / carers staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) 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 Head Teachers to such extent as is reasonable, to regulate the behaviour of students 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 Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Head Teacher and Senior Leaders:

• The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.

• The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).

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

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

The Online Safety Group Nottinghamshire County Council ICT services (as required) The Tackling Emerging Threats to Children Team (NCC)

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

Online Safety Coordinator

Leads on Online Safety

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

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

• provides training and advice for staff

• liaises with the Local Authority / relevant body

• liaises with school technical staff

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

Incidents regarding students will be dealt with on an individual basis and according to the needs of those involved.

The member of staff dealing with incidents will be organised / delegated by the Online Safety Coordinator for students.

o incidents regarding others (including staff) will be dealt with according to school procedures (e.g. disciplinary)

o the member of staff dealing with incidents will be organised by the Head Teacher for others (including staff)

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

• attends relevant meetings of Governors

• reports regularly to Senior Leadership Team

This role will be taken on by Cathy Clay, Head Teacher.

Resource Manager and Subject Leader for Computing:

The Resource Manager, with support if required from the Subject Leader for Computing, is responsible for ensuring:

• that Derrymount's technical infrastructure is secure and is not open to misuse or malicious attack

• that Derrymount meets required online safety technical requirements and any Local Authority Group Online Safety Policy / Guidance that may apply.

• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

• the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)

• that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

• that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher; Online Safety Coordinator for investigation / action / sanction 6

• that monitoring software / systems are implemented and updated as agreed in school policies Teaching and Support Staff Are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices

• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

• they report any suspected misuse or problem to the Head Teacher / Senior Leader ; Online Safety Coordinator for investigation / action / sanction

• all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems

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

• students understand and follow the Online Safety Policy and acceptable use policies

• students 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 students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

These are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Students: As appropriate to their level of need and understanding:

• are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement

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

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools' Online Safety Policy covers their actions out of school, if related to their membership of the school

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, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events

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

• their children's personal devices in the school (where this is allowed) Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices.

Policy Statements Education

Students The education of students in online safety is an essential part of the schools' online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

• Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

• Students 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.

• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (The Counter Terrorism and Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet.)

• Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school, as appropriate to their needs

• 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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

Education – Parents / Carers Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Derrymount will therefore seek to provide information and awareness to parents and carers through:

• Letters, newsletters, web site

• Parents / Carers evenings / sessions

• High profile events / campaigns e.g. Safer Internet Day

• Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

• All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

• It is expected that some staff will identify online safety as a training need within the performance management process.

• The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

• This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

• The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / or another relevant organisation.

• Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons). School Technical Security (including filtering and passwords). Derrymount will be responsible for ensuring that our school infrastructure / network is as safe and secure as is reasonably possible and that:

• users can only access data to which they have right of access

• no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)

• access to personal data is securely controlled in line with the school's personal data policy

• logs are maintained of access by users and of their actions while users of the system

• there is effective guidance and training for users

• there are regular reviews and audits of the safety and security of school computer systems

• there is oversight from senior leaders and these have impact on policy and practice Responsibilities The management of technical security will be the responsibility of the Resource Manager. Technical

Security Derrymount will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

• Derrymount's 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 academy technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data

• Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff

• All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Resource Manager and will be reviewed, at least annually, by the Online Safety Coordinator.

• Users will be made responsible for the security of their username and password 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. (See Password section below)

• The Resource 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

• Mobile device security and management procedures are in place (for school provided devices and / or where mobile devices are allowed access to school systems)

• Derrymount's technical staff member regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement

• Remote management tools (eg Impero) are used by staff to control workstations and view users activity

• An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Resource Manager.

o Users should put any concerns in writing (preferably via email) to the Online Safety Coordinator / Resource Manager as soon as possible.

o They will deal with the incident in the appropriate manner.

• Provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems:

Long term supply teachers if they are working in the school on a long placement will be given their own accounts.

They will be issued with a school email account and log on for work purposes.

Their account will be deleted / disabled as their placement finishes.

• Extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school:

Devices issued to teachers (e.g. laptops) may be used out of school

iPads must have appropriate restrictions, passcodes and filtering set

o Devices used at home may be subject to checks by SLT if required by use of Impero.

• Allowing or forbidding staff to download executable files and installing programmes on school devices:

Staff must not download anything that is illegal.

Staff must not download anything they suspect may contain a virus Staff should speak to the Resource Manager for further guidance.

To download iPad apps, please speak to the Resource Manager as the system is centrally managed

- All removable media (e.g. memory sticks / CDs / DVDs) will be encrypted automatically.
- School data can only be taken off the school site if it is encrypted or otherwise secured
- o If a virus is suspected, the device must not be used within school Password Security A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

• All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Resource Manager and will be reviewed, at least annually, by the Online Safety Coordinator

• All Derrymount's networks and systems will be protected by secure passwords and in a secure format (upper and lower case, numbers and special characters at least 8 characters long)

• The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Head Teacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.

• All users (adults and young people) will have responsibility for the security of their username and password 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

• Passwords for new users, and replacement passwords for existing users will be allocated by the Resources Manager Staff Passwords

• All staff users will be provided with a username and password by the Resource Manager who will keep an up-to-date record of users and their usernames.

• The password should be secure and changed on a regular basis (at least annually for staff) and in a secure format (upper and lower case, numbers and special characters at least 8 characters long)

• Office 365 passwords will be changed as requested by the system

• Passwords should not be shared with other members of staff unless necessary (e.g. PA to Head Teacher)

• Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

• Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

• Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school

• In the event of a suspected breach, a password reset should be sought immediately from the Resource Manager Student Passwords

13 • All users will be provided with a username and password by the Resource Manager who / which will keep an up-to-date record of users and their usernames.

• Users will not be required to change their password, unless there has been a breach

• Students will be taught the importance of password security

• The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Audit / Monitoring / Reporting / Review The Resource Manager will ensure that full records (manual or automated) are kept of:

• User IDs and requests for password changes

• User logins

• Security incidents related to this policy

Filtering The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

• Derrymount maintains and supports the managed filtering service provided by our IT provider

• In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher (or other nominated senior leader).

• Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems

• Any filtering issues should be reported immediately to the filtering provider.

• Requests from staff for sites to be removed from the filtered list will be considered by the Resource manager and the Online Safety Coordinator, to ensure protection for the Resource Manager or any other member of staff, should any issues arise re unfiltered access. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Coordinator.

Education / Training / Awareness Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through:

• the Acceptable Use Agreement

• induction training

• staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Monitoring No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Refer to 'Keeping Children Safe in Education' 2021 for further guidance.

Mobile Technologies The use of mobile technologies within school should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, GDPR policies, 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, students and parents/carers gives consideration to the use of mobile technologies.

	School Devices			**Personal Devices**		
Allowed in school	**School owned for single user**	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Full internet access				Yes stored securely in the office.	Yes	Yes
Internet only						
No internet access					Yes	Yes

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices.

• 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)

• Derrymount 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

Authorised device – purchased by the student/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Visitors' devices: Should be switched off or on silent; Must not be in use around students, unless permission has been given by the Head Teacher (e.g. school shows); Must not be used to take photos or videos of students or staff, unless permission has been given by the Head Teacher (e.g. school shows)

• Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user

• All Derrymount devices are subject to routine monitoring

• Pro-active monitoring has been implemented to monitor activity School owned / provided devices:
• Who they will be allocated to o All teachers will be allocated a laptop and an iPad

All pupils will be allocated a laptop and a number of iPads depending on the needs of the pupils in the class.

• Where, when and how their use is allowed – times / places / in school / out of school

Teachers may take their allocated devices off site.

Devices within school should only be used for work purposes. Devices used out of school may be used for purposes other than work, but these must not in any way be used for something that is inappropriate.

Inappropriate use may result in disciplinary action being taken.

• If personal use is allowed. Support staff may only take a device out of school with permission from SLT.

• Taking / storage / use of images

o Images may be taken of pupils but may only be used (e.g. in publications) with parental permission

- Images must be removed from portable devices (e.g. iPads, cameras) as soon as possible and stored on the school server.
- It must not be possible to identify a pupil (e.g. their name) from the image saved

o Staff must only use school devices to take images of pupils. Use of personal phones for this purpose is prohibited

• Liability for damage

o Within school, damage will be covered under Derrymount's policy

o Care must be taken to limit this damage

o Protective covers and screens must be used to prevent this damage occurring

o If staff remove devices from the school site, then they must ensure that their personal home insurance will cover loss or damage. If not, they will be liable for the cost of repair or replacement.

• Staff training

o Staff will receive relevant training as required 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

• Derrymount 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)

• Derrymount 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

• Derrymount 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

• Derrymount is not responsible for the day-to-day maintenance or upkeep of the users' personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Personal devices: • Restrictions on where, when and how they may be used in school.

o Should be switched off or on silent and must not be on the person during lesson time, unless permission of the Head Teacher or other Senior Leader has been sought (e.g. family emergency) (staff)

o Can be used in staff areas at breaks and lunchtimes only (staff)

o Should be switched off or on silent (visitors)

o Must not be in use around students, unless permission has been given by the Head Teacher (e.g. school shows) (visitors)

o Must not be used to take photos or videos of students or staff, unless permission has been given by the Head Teacher (e.g. school shows) (visitors)

o • Storage o Must be locked / stored away from the classroom

o Student devices are handed over on entry to school and stored securely until the end of the day • Whether staff will be allowed to use personal devices for school business

o Staff may use personal devices for agreed aspects of school business, but this is not encouraged

o It is not recommended that staff have work emails on their personal devices

o Staff should try to send work emails only during work times. Where emails are sent in the evenings, a response is never expected at that time.

• **Levels of access to networks / internet (as above)**

o Personal devices will be permitted access to the internet

• Technical support o Technical support for personal devices is not available

• **The right to take, examine and search users devices in the case of misuse**

o In the event of misuse being suspected, it is possible that the Head Teacher will examine and search devices

o This may result in disciplinary action

• **Taking / storage / use of images**

o The use of personal devices for taking images of pupils is not allowed (staff)

o Parents – Must not be in use around students, unless permission has been given by the Head Teacher (e.g. school shows)

o Parents – Must not be used to take photos or videos of students or staff, unless permission has been given by the Head Teacher (e.g. school shows)

• Liability for loss/damage or malfunction following access to the network

o Derrymount is not liable or responsible for any personal devices brought onto the school premises

• **Identification / labelling of personal devices**

o Personal devices should be identifiable

o They must not be left lying around school

o They should have password protection

• **How visitors will be informed about school requirements**

o Visitors will be informed through an information leaflet on entry to school

o Should be switched off or on silent

o Must not be in use around students, unless permission has been given by the Head Teacher (e.g. school shows)

o Must not be used to take photos or videos of students or staff, unless permission has been given by the Head Teacher (e.g. school shows)

• **How education about the safe and responsible use of mobile devices is included in the school** Online Safety education programmes

o Online safety training will be refreshed every three years 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.

19 • **Confiscation and searching**- 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

• Printing from personal devices will not be possible

This refers to the searching for and of electronic devices and the deletion of data / files on those devices.

Students are allowed to bring mobile phones or other personal electronic devices to school and store them securely in the office and use them only within the rules laid down by the school. The sanctions

for breaking these rules will be: warning, contact with parents, further sanction, a ban Authorised staff (HT or member of SLT) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

• Searching with consent - Authorised staff may search with the pupil's consent for any item

• Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) In carrying out the search, the authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training. The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched. The authorised member of staff carrying out the search should be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ pupil being searched. There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff. The person conducting the search may not require the student/ pupil to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags. A students' possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff. The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do. Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for. Electronic devices An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules). The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage. If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Examples of illegal activity would include:

• child sexual abuse images (including images of one child held by another child)

• adult material which potentially breaches the Obscene Publications Act

• criminally racist material

• other criminal conduct, activity or materials Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation. The school considers its duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There will be arrangements in place to support such staff as required.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the flow chart in the main School Template Policies document or on the NSCB website. **Deletion of Data** Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules). If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

Audit / Monitoring / Reporting / Review The responsible person (Online Safety Coordinator) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by the Online Safety Governor at least annually. This policy will be reviewed by the Head Teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Use of digital and video images The development of digital imaging technologies has created significant benefits to learning, allowing staff and students 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.

Derrymount will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

• Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press

• In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Students' work can only be published with the permission of the student (if appropriate) and parents or carers.

• Parents / carers will need to complete a photography consent form (in line with GDPR policies) 24 Data Protection With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) 2016. As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the GDPR policies within school. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

• It has a Data Protection Policy

• It has paid the appropriate fee to the Information Commissioner's Office (ICO)

• It has appointed a Data Protection Officer (DPO)

• 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

• Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay

• The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice

• Where special category data is processed, a lawful basis and a separate condition for processing have been identified

• Data Protection Impact Assessments (DPIA) are carried out

• It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers

• Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller

• There are clear and understood data retention policies and routines for the deletion and disposal of data

• There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible

• Consideration has been given to the protection of personal data when accessed using any remote access solutions

• Derrymount has a Freedom of Information Policy which sets out how it will deal with FOI requests

• All staff receive data handling awareness / data protection training and are made aware of their responsibilities

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, memory stick or any other removable media:

• 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 / academy policy (below) once it has been transferred or its use is complete.

Where possible, staff should use One Drive online storage linked to their Office 365 work account. This is the preferred method of file storage.

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:

COMMUNCIATION TECHNOLOGIES	STAFF OR OTHER ADULTS				STUDENTS			
	Allowed	Allowed At Certain Times	Allowed For Selected Staff	Not Allowed	Allowed	Allowed At Certain Times	Allowed with staff permi-ssion	Not Allowed
Mobile phones may be brought to the school.	■				■			
Use of mobile phones in lessons.				■				■
Use of mobile phones in social time.	■							■
Taking photos on mobile phones / cameras.				■				■
Use of other mobile devices eg tablets/ gaming devices.							■	
Use of personal email addresses in school.		■						■
Use of school email for personal emails.				■				■
Use of messaging apps.		■						■
Use of social media			■					■
Use of blogs.		■					■	

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

• Derrymount's official email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. 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 students or parents / carers (email, social media, chat, blogs 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 social media must not be used for these communications

• Students will be provided with individual school email addresses for educational use where the programme of study requires (e.g. Functional Skills ICT)

• Students should be taught about online safety 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

Social Media All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority group liable to the injured party. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

• Ensuring that personal information is not published

• Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues

• Clear reporting guidance, including responsibilities, procedures and sanctions

• Risk assessment, including legal risk The school does not have a social media account. If consideration is given to this in the future, then guidance will be produced accordingly.

Behaviour • The school name should not be listed as a place of work on personal social media accounts

• Staff must not add, request or accept friend requests from pupils

• It is recommended that staff are not 'friends' with parents/carers on social media sites

• Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use personal social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff, pupils or any school business. Staff must ensure that confidentiality is maintained on personal social media even after they leave the employment of the school

• If a journalist makes contact about posts made using social media staff must contact the Head Teacher to discuss the matter 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 through school technology is not permitted (unless by SLT for a specific purpose). Personal use 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 School staff should ensure that:

• No reference should be made in social media to students, parents / carers or school staff

• They do not engage in online discussion on personal matters relating to members of the school community

• Personal opinions should not be attributed to the school or local authority

• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information Use of images

• Under no circumstances should staff share or upload student pictures to their social media accounts

• If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately

Managing your personal use of Social Media:

• "Nothing" on social media is truly private

• Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts

• Check your settings regularly and test your privacy

• Keep an eye on your digital footprint

• Keep your personal information private

• Regularly review your connections – keep them to those you want to be connected to

• When posting online consider; Scale, Audience and Permanency of what you post

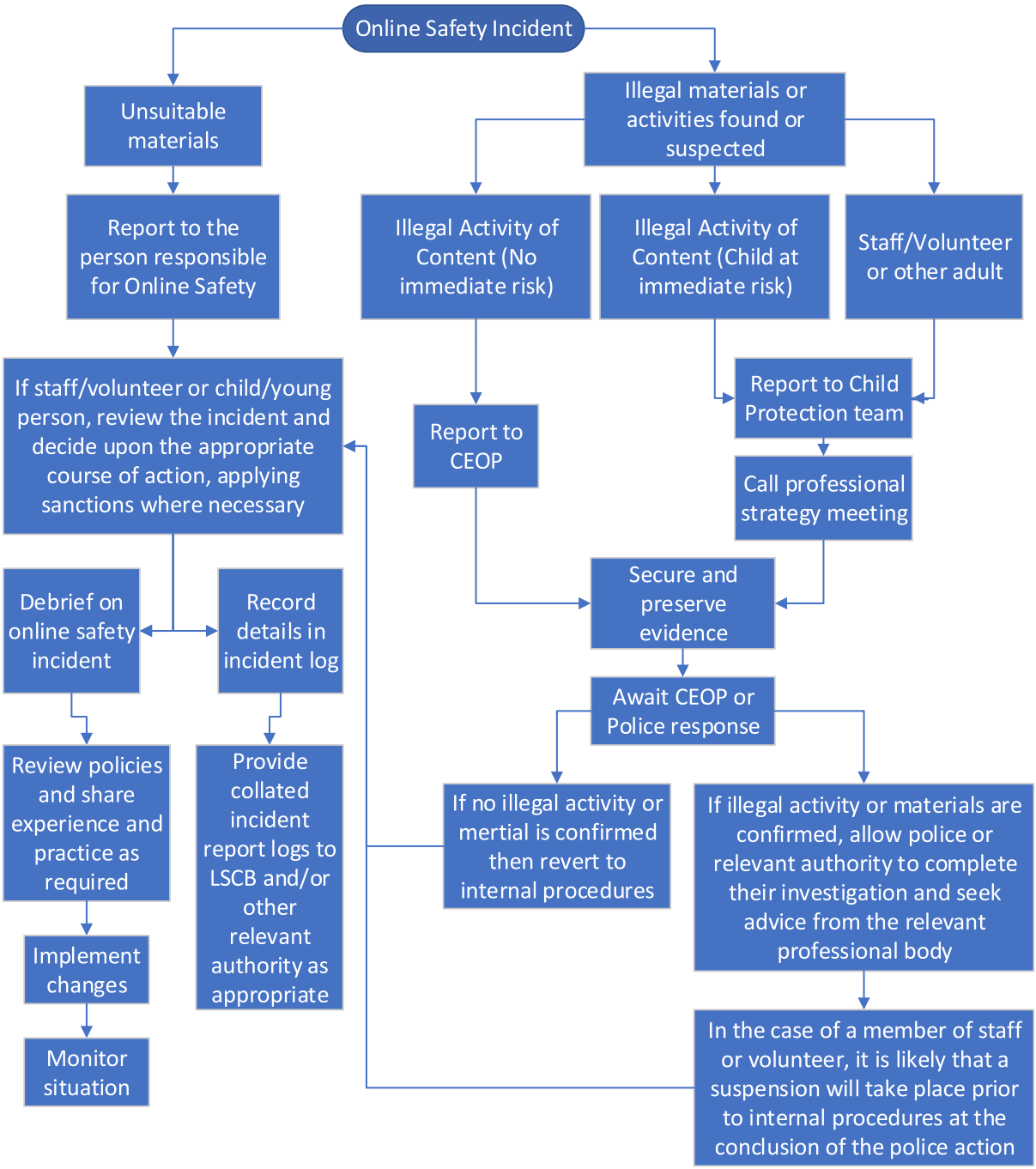
• If you want to criticise, do it politely

• Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?

• Know how to report a problem

Dealing with unsuitable / inappropriate activities Derrymount School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Un-acceptable	Un-acceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.					
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					
Pornography Promotion of any kind of discrimination threatening behaviour, including promotion of physical violence or mental harm					
Promotion of extremism or terrorism					
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of our school or brings Derrymount into disrepute.					
Using school systems to run a private business.					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					
Infringing copyright					
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					
Creating or propagating computer viruses or other harmful files					
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping /commerce					
File sharing					
Use of social media					
Use of messaging apps					
Use of video broadcasting e.g. You tube (this does not refer to watching videos for educational purposes)					


Online Safety Incident
Unsuitable materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity of Content (No immediate risk)
Illegal Activity of Content (Child at immediate risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Await CEOP or Police response
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
If no illegal activity or mertial 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
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents It is hoped that all members of our school community will be responsible users of digital technologies, who understand and follow our 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:

o Internal response or discipline procedures o Involvement by Local Authority or national / local organisation (as relevant).

o 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:

o incidents of 'grooming' behaviour

o the sending of obscene materials to a child

o adult material which potentially breaches the Obscene Publications Act

o criminally racist material

o promotion of terrorism or extremism o 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: The following actions by pupils or staff could result in a number of actions or sanctions (list not exhaustive):

• Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)

• Unauthorised use of non-educational sites during lessons

• Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device

• Unauthorised / inappropriate use of social media / messaging apps / personal email

• Unauthorised downloading or uploading of files

• Allowing others to access school network by sharing username and passwords

• Attempting to access or accessing the school network, using another student's 's account

• Attempting to access or accessing the school network, using the account of a member of staff

• Corrupting or destroying the data of other users

• Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
• Continued infringements of the above, following previous warnings or sanctions

• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school • Using proxy sites or other means to subvert the schools' filtering system

• Accidentally accessing offensive or pornographic material and failing to report the incident

• Deliberately accessing or trying to access offensive or pornographic material

• Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

• Breaching copyright or licensing regulations

• Deliberate actions to breach data protection rules (staff only)

• Actions which could compromise the staff members professional standing (staff only)

Possible actions or sanction FOR PUPILS may include (list not exclusive):

• Being dealt with by the class staff# • Referral to SLT / Head Teacher • Contact with parents / carers
• Referral to the police

• Referral to technical support staff

• Removal of network / internet access

• Warning

• Further sanction e.g. behaviour incident log, safeguarding log, suspension

Possible actions or sanction FOR STAFF may include (list not exclusive):

• Referral to Line Manager

• Referral to Head Teacher

• Referral to Local Authority / HR

• Referral to the police

• Referral to technical support staff

• Warning

• Suspension

• Disciplinary action (which may result in dismissal)

Acknowledgements This policy template has been provided by SWGfL (2018). Nottinghamshire County Council advocates the use of this policy to base a school specific policy on.

Appendices

1 Student Acceptable Use Agreement

2. Parent / Carer Acceptable Use Agreement

3. Staff (including volunteers and students on placement) Acceptable Use Policy Agreement

4. Record of reviewing devices / internet sites (responding to incidents of misuse)

5. Reporting Log

6. Training Needs Audit Log

Student Acceptable Use Agreement

This is how we stay safe when we use computers:

• I will ask a teacher or suitable adult if I want to use the computers / tablets

• I will only use activities that a teacher or suitable adult has told or allowed me to use

• I will take care of the computer and other equipment

• I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

• I will tell a teacher or suitable adult if I see something that upsets me on the screen

• If I choose to bring my phone to school, I will hand it over as I arrive into school

• I will keep my password safe and secure

• I will use the rules set down by my teacher and will not use anything that I have been told I cannot

• I will not take or distribute images of anyone without their permission

• I will not download or install anything onto the school computers or tablets

• I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): _____

Signed (parent): _____ Date: _____

Parent / Carer Acceptable Use Agreement

Parent / Carers Name: _____

Student Name: _____

As the parent / carer of the above students, I give permission for my son / daughter to have access to the internet and to ICT systems at school. I understand that I have discussed (and where appropriate, my son / daughter has signed) the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: Date:

Staff (including volunteers and students on placement)

Acceptable Use Policy Agreement I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

• I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured

• I will only use social networking sites in school in accordance with the school's policies

• I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner

• I will not engage in any on-line activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school

equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses

• I will not use personal email addresses on the school ICT systems

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will ensure that my data is regularly backed up, in accordance with relevant school policies

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies, without permission

• I will not disable or cause any damage to school equipment, or the equipment belonging to others

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school data protection policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage

• I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority

• I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos) I understand that I am responsible for my actions in and out of the school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors

and / or the Local Authority and in the event of illegal activities the involvement of the police I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: _____ Role: _____ Signed: _____ Date: _____

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group:

_____Date:_____

Reason for investigation:

_____

_____

_____

_____

Details of first reviewing person Name: _____

Position: _____

Signature: _____

Details of second reviewing person Name: _____

Position: _____

Signature: _____

Name and location of computer used for review (for web sites)

_____

_____

_____ Web site(s) address / device Reason for concern Conclusion and Action proposed or taken.

REPORTING LOG Group:						
DATE	TIME	INCIDENT	ACTION TAKEN		INCIDENT REPORTED BY	SIGNATURE
			WHAT?	BY WHO?		