Rosstulla School



E-Safety Policy

 Governors approved January 2022

Chairperson signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CHAPTERS**

1. Purpose and Rationale
2. Development/Monitoring and Review of Policy
3. Roles and Responsibilities
4. Education & Training
5. Mobile Technologies
6. Use of Digital and Video Images
7. Data Protection
8. Communication

**APPENDICES**

Appendix 1 – Securus

Appendix 2 - Responding to Incidents of Misuse Chart

Appendix 3a - Staff and Volunteer Acceptable Use Policy Agreement

Appendix 3b - Student Acceptable Use Agreement – Secondary

Appendix 3c – Student Acceptable Use Agreement – Primary & Nursery

Appendix 3d - Acceptable Use Agreement Parent/Carer

Appendix 4 - Social Media Policy for School Staff

Appendix 5 – Digital Permission Form

Appendix 6 – Seesaw Permission Form

1. **PURPOSE and RATIONALE**

**The Purpose of this policy statement is to**:

* ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
* provide staff and volunteers with the overarching principles that guide our approach to online safety
* ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The policy statement applies to all staff, volunteers, children and young people at Rosstulla School.

**We believe that**:

* children and young people should never experience abuse of any kind
* children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.

**We recognise that**:

* the online world provides everyone with many opportunities; however, it can also present risks and challenges
* we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
* we have a responsibility to help keep children and young people safe online, whether or not, they are using Rosstulla School’s network and devices
* all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
* working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people’s welfare and in helping young people to be responsible in their approach to online safety.

**We will seek to keep children and young people safe by**:

* appointing an online safety coordinator (Vice Principal /Designated Teacher)
* providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults and our acceptable use agreement
* supporting and encouraging the young people using our service to use the internet, social media and mobile technology in a way that keeps them safe and shows respect for others
* supporting and encouraging parents and carers to do what they can to keep their children safe online
* developing an online safety agreement for use with young people and their parents/carers
* developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
* reviewing and updating the security of our information systems regularly
* ensuring that usernames, logins, email accounts and passwords are used effectively
* ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
* ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
* providing supervision, support and training for staff and volunteers about online safety
* examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

This policy applies to all members of our school community (including staff, governors, students, parents/carers, visitors, volunteers) who have access to and are users of Rosstulla School’s digital technology systems.

1. **DEVELOPMENT / MONITORING / REVIEW OF POLICY**

This online safety policy has been developed by a working group (E-Safety Team) made up of:

* Vice Principal (Online Safety Lead)
* C2K manager
* ICT Coordinators

*Consultation with relevant KS staff has taken place*

Schedule for Development/Monitoring/Review

5

|  |  |
| --- | --- |
| This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on: | Insert date |
| The implementation of this online safety policy will be monitored by:  | Vice Principal (Online Safety Lead) ICT Co-ordinators, C2K Manager, Senior Leadership Team,  |
| Monitoring will take place at regular intervals: | Annually |
| The Board of Governors will receive a report on the implementation of the online safety policy, generated by the Vice Principal | Annually (end of Term 3) |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | June 2022 |
| Should serious online safety incidents take place, the following external agencies should be informed: | Child Protection School Support Team (CPSS). Gateway, PSNI |

The school will monitor the impact of the policy using:

Internal monitoring data for network activity via \*Securus will be carried out regularly by the C2K manager. Any relevant documents will be stored in pupil’s yellow folders. Other incidents will also be logged using SIMS under the category E-Safety.

* Surveys/questionnaires of pupils / parent & carers / staff

(\*See appendix 1)

1. **ROLES and RESPONSIBILITIES**

The following section outlines the online safety roles and responsibilities of individuals and groups within Rosstulla School community.

**Governors**

Governorsare responsible for the approval and reviewing the effectiveness of the online safety policy.

The role of Rosstulla School’s Designated Online Safety Governor (Mrs Lynda Stewart) will include:

* attendance at E-Safety Team meetings (termly)
* regular monitoring of online safety incident logs
* reporting to relevant Board of Governor meetings

**Principal and Senior Leaders**

* The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community,
* The Principal and members 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 Appendix 1)
* The Principal and Senior Leaders are responsible for ensuring that staff receive appropriate training to enable them to carry out their online safety roles and to train other colleagues.
* The Principal and 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 to support to those colleagues who take on important monitoring roles
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead (Vice Principal)

**Online Safety Lead**

* leads the E-Safety Team
* takes day to day responsibility for online safety issues and has a leading role in monitoring and reviewing the E-Safety policy
* ensures that all staff are aware of E-safety procedures.
* Liaises with the SLT/ICT Co-ordinators/C2K Manager in identifying/sourcing training and advice for staff
* receives reports of online safety incidents via Securus and creates a log of incidents via SIMs to inform future online safety developments.
* meets termly with E-Safety Team (and Designated Governor)to discuss current issues and review incident logs
* reports regularly to Senior Leadership Team

**C2K Manager**

* Set up and manage C2K staff and pupil accounts.
* can change staff and pupil access levels
* Monitors Securus for potential problems and reports these to the appropriate staff member and online safety lead
* Liaise with C2K/Capita and update staff on necessary communications from C2K.
* **C2K are responsible for ensuring:**
* that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* that users may only access the networks and devices through a properly enforced password protection policy
* the filtering policy is applied and updated on a regular basis
* that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders; Online Safety, C2K Manager for investigation/action/sanction

**Teaching and Support Staff**

Are responsible for ensuring that:

* they have an up-to-date awareness of online safety matters and of the E-Safety policy & procedures
* they have read and understood the Staff Acceptable Use policy/agreement (Appendix 2)

they report any suspected misuse or problem (See Appendix 1) .

* 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 throughout the curriculum and other activities
* pupils understand*, to the best of their abilities*, the importance of online safety and follow the Acceptable Use policy
* they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices

**Designated Safeguarding Teacher(s)**

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
* online-bullying

**E-Safety Team**

The E-Safety Team will be made up of Principal, Online Safety Lead (Vice Principal), ICT coordinators, C2K Manager and will assist the Online Safety Lead with:

* Monitoring & reviewing E-Safety policy.
* monitoring network/internet/filtering/incident logs via Securus
* consulting stakeholders – including parents/carers and the students/pupils about the online safety provision

**Students:**

* are responsible for using Rosstulla School’s digital technology systems in accordance with the student Acceptable Use Agreement (Appendix 2)
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials. They should also be aware of the reporting procedures (and know who to speak to if they need help)
* will be familiar with the rules regarding the use of mobile devices, digital cameras, taking/use of images and on online-bullying.

**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. Rosstulla will endeavour to help parents understand these issues through the Safer Schools NI App and various platforms (e.g. parents’ evenings, newsletters, website, social media etc.*).* *.* Parents and carers will be encouraged to support Rosstulla 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/social media pages/Seesaw and on-line student/pupil records
* their children’s personal devices (through close monitoring & supervision)

6

1. **EDUCATION and TRAINING**

**Students:**

The education of pupils in online safety/digital literacy is an essential part of Rosstulla’s online safety provision. Children and young people need help and support 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:

* Rosstulla will plan and provide opportunities within a range of curricular areas, to teach E-Safety.
* Key online safety messages will be reinforced as part of a planned programme including LLW, Circle Time, assemblies.
* Students should be supported to ensure that they are safe from online threats.
* Students should be encouraged to adopt safe and responsible use both within and outside school.
* Where students are allowed to search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

**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 online 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.

Rosstulla School will seek to provide information and awareness to parents and carers through:

* SaferSchoolsNI App.
* Curricular activities
* Signposting to the helpful websites/publications via our website, Seesaw and social media pages
* Parents/carers evenings/sessions / Family Learning sessions
* High profile events/campaigns e.g. Safer Internet Day

**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:

* Each year, E-safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out annually. E-safety updates and guidance documents will be shared with staff as appropriate.
* All new staff will receive a copy of the E-safety policy as part of their induction pack.
* The Online Safety Lead will provide advice/guidance/training to individuals as required.
* Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

**Governors**

* Governors are required to complete online awareness training (as directed by Education Authority)
* Governors will also be invited to any relevant training/information sessions for staff or parents / carers

**Technical –Infrastructure/equipment, filtering and monitoring**

* Servers, wireless systems and cabling are securely located and physical access is restricted
* All users will have clearly defined access rights to school technical systems and devices
* All users will be provided with a username and secure password by (C2K) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
* Pupil passwords are reset at start of each year and distributed to form staff who then assist pupils in updating this to a secure password.
* The “master/administrator” passwords for the school systems, used by the Network Manager are available to the Principal or other nominated senior leader via C2K on request
* C2K 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)
* IPads are monitored and apps downloaded and updated via the MDM, Mobile Device Management System, by the school Technician in consultation with ICT Coordinators and C2K lead.
* Internet access is filtered for all users by C2K. Requests for changes to filtering levels can be made through C2K lead who then instructs C2K to adapt accordingly if appropriate.
* Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet this is provided by C2k and Securus
* C2K has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
* C2K Lead and Online Safety Officer regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
* C2K is responsible for ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
* An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. (See Acceptable Use Policy)
* Short term substitute staff will be given access to the system via guest passwords. Short term staff will be informed that all system access is monitored by Securus via their login cards.
* Long term substitute staff will be issued with a substitute teacher username and password for the duration of their employment.
* An agreed policy is in place (Appendix 2) regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
* An agreed policy is in place (Appendix 2) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
* Removable media eg memory sticks should not be used to transport personal data. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
* All data relating to school /pupils should be stored securely on the cloud via Office 365.
1. **MOBILE TECHNOLOGIES**

Mobile technology devices may be school owned/ or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilizing the school’s wireless network. The device then has access to the wider internet including cloud-based services such as email and data storage.

**All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational**.

* The school Acceptable Use agreements for staff, students and parents/carers.
* Pupils are discouraged from bringing their own devices to school.
* The school allows:

|  |  |  |
| --- | --- | --- |
|  | School Devices | Personal Devices |
|  | **School owned for single user** | **School owned for multiple users** | **Authorised device** | **Student owned** | **Staff owned** | **Visitor owned** |
| Allowed in school | ***Yes*** | ***Yes*** | ***Yes*** |  | *Yes* | *Yes* |
| Full network access | ***Yes*** | ***Yes*** | ***Yes*** |  | *Filtering limited by C2K access* | *No* |
| Internet only | ***Yes*** | ***Yes*** | ***Yes*** |  | *Yes via C2K* | *No unless specifically required for training needs* |

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

* All school mobile devices are controlled though the use of Mobile Device Management software.
* 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 Rosstulla or by an authorised user
* All school devices are subject to routine monitoring by staff they have been assigned to and via the MDM

*When personal devices are permitted:*

**Staff:**

* Personal devices are brought into Rosstulla entirely at the owner’s risk. Liability for any loss or damage resulting from the use of the device in school, lies with the owner.
* 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 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.

**Pupils**

* + 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.
	+ On arrival at school all personal devices should be handed to the form teacher and are stored securely until return at the end of the school day.
	+ 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 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

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

* Visitors should be provided with information about how and when they are permitted to use mobile technology in line with 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 the school
	+ Devices must be in silent mode on the school site and on school buses
* 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.
* The school will ensure that 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 pupils 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
* Devices may be used in lessons in accordance with teacher direction
	+ 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
1. **USE OF VIDEO AND DIGITAL IMAGES**

The development of digital imaging technologies has created significant benefits to learning. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet.

* 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/Seesaw(Appendix 4 and 5)
* 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 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.
* Student’s work can only be published with the permission of the student and parents/ carers.
1. **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**). Rosstulla School’s Data Protection Policy is available on request from main office.

**When personal data is stored on any mobile device:**

* data must be stored in online cloud locations.
* device must be password protected.
* device must be protected by up-to-date virus and malware checking software.

16

* data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

**Staff must ensure that they**:

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

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

* The **C2K email service** may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
* Users must immediately report– in accordance with the school’s 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 must be professional in tone and content. These communications should only take place on official C2K or Seesaw systems. Staff should not access the Seesaw app in a public setting - only in their home setting and on private Wi-Fi connection. Personal email addresses, text messaging or social media must not be used for these communications.
* 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.

**Students’ emails**:

* Students may only use approved class email accounts (through C2K system).
* Passwords will be kept by class teacher.
* Students will be taught not to reveal personal details of themselves or others in email communication.
* Incoming emails to class email addresses should only be opened if the author is known.
* Any offensive emails must be reported to the teacher immediately.

**Staff emails**:

* Personal email addresses (e.g Gmail, Hotmail, Yahoo etc.), should not be shared with any parent/carer or student.
* Any communication between staff and parent/carer, should be carried out through C2K or Seesaw.
* Any offensive emails must be reported to the Principal and Online Safety Lead.
* All communications between adults and children should take place within clear, explicit boundaries, and where age appropriate, with prior consent of the parent/carer. Adults will not share any personal information with a child, and they should not request or respond to any personal information from the child other than that which might be appropriate as part of their professional role. Adults must ensure that all communications are transparent and open to scrutiny.
* Staff are advised not to use memory sticks to transfer data but to store data securely in online locations.

|  |  |  |
| --- | --- | --- |
| Communication Technologies | Staff and other adults | Students/Pupils |
|  | Allowed  | Allowed at Certain Times | Allowed for selected staff | Not allowed | Allowed  | Allowed at Certain Times | Allowed for selected pupils | Not allowed |
| Mobile phones may be brought to the school | X |  |  |  | X |  |  |  |
| Use of mobile phones in lessons |  |  |  | X |  |  |  | X |
| Use of mobile phones in social time | X |  |  |  |  |  |  | X |
| Taking photos on mobile phones/cameras |  |  |  | X |  |  |  | X |
| Use of other mobile devices e.g. tablets, gaming devices |  | X |  |  |  | X |  |  |
| Use of personal email addresses in school, or on school network |  | X |  |  |  |  |  | X |
| Use of school email for personal emails |  |  |  | X |  |  |  | X |
| Use of messaging apps |  | X |  |  |  |  |  | X |
| Use of social media |  | X |  |  |  |  |  | X |

**Social Media**

Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

Rosstulla has a duty of care to provide a safe learning environment for pupils and staff. Our school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, staff and the school through the implementation of our Social Media Policy (Appendix 3)

Children, Young People &Families -A Parent’s Guide to Technology(UKSIC)http://www.saferinternet.org.uk/advice-and-resources/a-parents-guideConnectSafelyhttp://www.connectsafely.orgDigizenhttp://www.digizen.orgKidSmarthttp://www.kidsmart.org.uk/Get SafeOnlinehttp://www.getsafeonline.org/Know ITAllhttp://www.childnet-int.org/kia/parents/Think UKnowhttp://www.thinkuknow.co.uk/Helping parents keep their children safe onlinewww.internetmatters

**APPENDIX 1**

**SECURUS**

Securus forms part of the e-Safety suite of tools available via the C2k network to safeguard children in their use of information systems and electronic communications.

Rosstulla has implemented Securus across their managed school network.

Securus monitors the screen display and keystrokes of students and guest users on C2K managed machines and triggers a capture if the content is listed in the database of inappropriate words and phrases

Logs of reported incidents: Relevant personnel will be informed of any Securus content needing further investigation and details of this will be recorded on SIMs as a Securus behaviour incident.

APPENDIX 2

RESPONDING TO INCIDENTS OF MISUSE FLOW CHART

Online Safety Incident

Unsuitable materials found or suspected

Illegal materials or activities found or suspected

Report to Online Safety Lead (Vice Principal)

Report to PSNI (under safeguarding protocol.

DO NOT DELAY, if you have any concerns, report them immediately

If person suspected is staff/volunteer or pupil, review the incident and decide upon appropriate course of action, applying sanctions where necessary

Secure and preserve evidence

Remember do not investigate yourself. Do not view or take possession of any videos/images

Call professional strategy meeting

Record details in incident log

Debrief on online safety incident

Review policies and share experiences and practice as required

Provide collated incident report to relevant authority as appropriate

Await PSNI response

If illegal activity or materials are confirmed, allow PSNI to complete their investigation and seek advice from CPSS

Implement changes

If no illegal activity or material is confirmed, then revert to internal procedures

Monitor

 situation

*Named person is responsible for the child’s wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate*.

In the case of a staff member or volunteer, it is likely that a suspension will take place at the point of referral to the PSNI, while PSNI and internal procedures are being undertaken

APPENDIX 3a

**Staff and Volunteer Acceptable Use Policy Agreement**

**School Policy**

New technologies have become integral to the lives of children and young people in today’s society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.  All users should have an entitlement to safe access to the internet and digital technologies at all times.

**This acceptable use policy is intended to ensure:**

* that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students’ learning and will, in return, expect staff and volunteers to agree to be responsible users.

**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, Seesaw, C2K network) 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, unless I have permission to do so. Where these images are published (e.g. on the school website/Social Media) 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 Social Media policy
* I will only communicate with students and parents / carers using official school systems C2K email, Seesaw. 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.
* 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. 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 to correspond on school matters.
* 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 securely stored on Office 365
* 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 install or attempt to install programmes/apps of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission is gained from the Principal to do so.
* 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 information GDPR policies.  Where digital personal data is transferred outside the secure local network, it must be password protected. 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.

**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 or the Education 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (PRINT)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (SIGNED)

 Date:

APPENDIX 3b

**Student Acceptable Use Agreement – Secondary**

Acceptable Use 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.

For my own personal safety:

* I understand that the school will monitor my use of the systems, devices and digital communications.
* I will keep my username and password safe and secure – I will not share it, 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 be aware of “stranger danger”, when I am communicating on-line.
* I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
* If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

* I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
* 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

* I will only use my own personal devices in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

* I should 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 try to download copies (including music and videos)
* When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

* I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
* I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action.  This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

**Student/Pupil Acceptable Use Agreement Form**

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

* I use the school systems and devices (both in and out of school)
* I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
* I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, commenting on social media, website etc.

Name of Student/Pupil:

Group/Class:

Signed:

Date:

APPENDIX 3c

**Acceptable Use Agreement Student – KS2**

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 adult has told or allowed me to use

* I will take care of computers/tablets 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
* I know that if I break the rules, I might not be allowed to use a computer/tablet

**Signed (child):**

APPENDIX 3d

**Acceptable Use Agreement Parent/Carer**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This acceptable use policy is intended to ensure**:

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the student acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

**PERMISSION FORM**

As the parent/carer of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (print student’s name), I give permission for \*him/her to have access to the internet and to ICT systems at school.

**For Secondary/KS2 Students (i.e. Years 4,5,6,7,8,9,10,11,12,13):**

I know that my \*son/daughter has signed an acceptable use agreement and has 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.

**For KS1/Foundation Stage (i.e. Years 1,2,3 & Nursery):**

I understand that the school has discussed 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 our children and 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 agreement.
* 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.

Parent/Carers Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (PRINT) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(SIGNED)

Date:

*\*delete as appropriate*

**APPENDIX 4**

**Social Media Policy for School Staff**

Contents

1. Introduction.....................................................................................................
2. Objectives.......................................................................................................
3. Responsibility and accountability.....................................................................
4. When using social media at any time ..............................................................
5. When using social media on behalf of the school............................................
6. When using social media as part of working with pupils and students ............
7. When using social media in staff’s wider professional life ...............................
8. When using social media in staff’s personal life ..............................................
9. Excessive use of social media at school .........................................................
10. Monitoring use of social media on school equipment ......................................
11. Disciplinary action over social media use ........................................................
12. If you have any concerns.................................................................................

**1 Introduction**

1. We actively encourage the responsible use of social media. Responsible use of social media can be positive for learning and teaching. It can also be personally enjoyable and beneficial.
2. This policy will make clear what standards are expected of anyone who works for the school and uses social media as well as what actions may be taken when it is considered a member of staff may have breached this policy.
3. This policy applies to all staff use of social media, including:
* on behalf of the school;
* as part of their work directly with pupils;
* in their wider professional lives; and
* in their personal lives.
1. In this policy, we define social media to mean:

‘Websites and applications that enable users to create and share content or to participate in social networking.’

1. In this policy, the word staff includes temporary and casual staff, agency staff, and volunteers during their time working with the school.
2. This policy works alongside other legislation, EA statutory guidance, and other school and EA policies such as Code of employee conduct, E safety framework policy and Acceptable use agreement. These all also apply where relevant.

**2 Objectives**

The purpose of this policy is to;

(a)  clarify what the school considers to be appropriate and inappropriate use of social networking by staff;

(b)  encourage social networking to be used in a beneficial and positive way;

(c)  safeguard staff, pupils, parents/carers and members of the public from abuse through social networking;

(d)  safeguard the reputation of the school, other schools, other organisations and employers from unwarranted abuse through social networking; and

(e)  set out the procedures that will be followed where it is considered that staff have inappropriately or unlawfully used social networking.

**3 Responsibility and accountability**

**Principal/Online Safety Lead:**

* should ensure that all existing and new staff are trained and become familiar with this policy and its relationship to the school’s standards, policies and guidance on the use of ICT and e-safety;
* should provide opportunities to discuss appropriate social networking use by staff and ensure that any queries raised are resolved swiftly;
* must ensure that any allegations raised in respect of access to social networking sites are investigated promptly and appropriately, in accordance with the school’s disciplinary procedure, code of conduct and internet safety guidelines; and
* should ensure there is a system in place for regular monitoring.

**School staff:**

* should ensure that they are familiar with the contents of this policy and its relationship to the school’s standards, policies and guidance on the use of ICT and e-safety;
* should raise any queries or areas of concern they have relating to the use of social networking sites and interpretation of this policy – with their line manager in the first instance; and
* must comply with this policy where specific activities or conduct is prohibited.

**School governors:**

* will review this policy and its application annually (or more frequently as required); and
* should ensure that their own behaviour is in line with that expected – as outlined in the governors’ code of conduct and in accordance with this policy.

**4 When using social media at any time**

* Staff must not place a child at risk of harm.
* Staff must always follow statutory and school safeguarding procedures when using social media.
* Staff must report all situations where any child is at potential risk by using relevant statutory and school child protection procedures.
* Staff must not allow their use of social media to affect their ability to do their job in any way.
* Social media relationships must be declared with other personal relationships or interests whenever necessary or appropriate.
* Staff must maintain the reputation of the school, its staff, its pupils, its parents, its governors, its wider community and their employers.
* Staff must not contribute or access any social media content which is illegal, discriminatory, sexual, or otherwise offensive when linked in any way to the school. This link could be, as examples, by identification with the school, during the working day, on school premises or when using school equipment. Such behaviours may also result in criminal proceedings.
* Staff must recognise that contributing or accessing any social media content which is illegal, discriminatory, sexual or otherwise offensive during personal use could lead to damage to their professional reputation or damage to the reputation of the school. This damage would breach the social media policy. And, again, such behaviours may also result in criminal proceedings.
* Staff must not use social media to criticise or insult their school, its staff, its pupils, its parents, its governors or its wider community.
* Staff should be aware that there are other, more appropriate, methods of raising valid concerns about their school and its staff.
* Staff must not use social media to harass, bully or intimidate any pupil, parent, member of staff, governor or other member of the wider school community.
* Staff must not breach school confidentiality.
* School staff must follow their school data protection responsibilities when using social media.
* Staff must not reveal any other private or confidential school matters when using any social media.
* Staff are responsible for their actions (and its consequences) whenever they use social media.
* Staff are responsible for all their social media content.
* Staff must understand that social media offers no guarantee of privacy and that any content they produce can be shared more widely by others. A member of staff’s professional reputation or the reputation of the school could be damaged by content, perhaps which was intended to be private, being shared more widely than intended.
* Staff would still be held responsible for any consequential breach of this policy as they were responsible for producing the original content.
* Staff are responsible for the configuration and use of any personal social media accounts they have. They are responsible for determining the level of security and privacy of all their social media content.
* Staff must raise all doubts, questions and concerns related to social media with school leaders.
* Staff must seek advice if they are not sure if any particular use of social media (or a related action) is appropriate or would potentially breach this policy.
* Staff cannot rely on their ignorance or lack of knowledge to defend any breach of this policy.

**5 When using social media on behalf of the school**

Some schools use social media as a communications channel for their school and to engage with their wider community.

* Staff must be given explicit permission to use social media on behalf of their school by a school leader.
* These staff must follow all related procedures when acting on behalf of the school.
* Staff must have separate user accounts for school use of social media.
* Staff must not use school social media for any personal discussions or for any individual personal matters even if initiated by other members of the school community. Users must be directed to more appropriate communication channels.

**6 When using social media as part of working with pupils and students**

Some schools are starting to use social media to engage with their own pupils to support learning.

1. Staff must ensure that all social media use when working with pupils is sanctioned by the school; only uses explicitly agreed social media; and, follows agreed policies and procedures.

**7 When using social media in staff’s wider professional life**

Social media is a useful tool for engaging and collaborating with the wider education community.

* Staff must be clear that their social media content is personal and not endorsed or supported by their school.
* Staff can identify their school where appropriate but cannot use account names, school branding or anything else that could imply that the content is official school content.
* Staff must be particularly careful to not reveal any details of staff, pupils, parents or other members of the school community that make it possible to identify any individuals.
* Staff must always use appropriate behaviour and language. As a guide, this should be similar to that which would be used when taking part in a face-to-face meeting with other education professionals.

**8 When using social media in staff’s personal life**

The personal use of social media must neither interfere with a member of staff’s ability to maintain their professional reputation nor impact on the reputation of the school.

* Staff must take all reasonable steps to ensure the proper separation of their professional and personal lives.
* Staff must not use school social networking accounts for personal content.
* Staff must respect the wishes and privacy of any other members of their school community with whom they have personal social media contact.
* Staff must not use personal social media with any child with whom they solely have, or have had, a staff/pupil relationship. This includes ex-pupils until they reach the age of 18.
* School staff can have social media contact with pupils or ex-pupils where other appropriate relationships exist. As examples, a pupil who is also a family member or a family friend. These relationships must be open and transparent. The member of staff can report these social media relationships to senior leaders for their own protection.
* Staff must retain any communications to pupils or ex-pupils rejecting any approaches made on social media and ensure that they are professional in tone. Staff must also consider reporting these to senior leaders to ensure transparency.
* Staff must not use personal social media with anyone with whom they solely have a staff/parent relationship.
* Staff at schools can often have more complex relationships than just being a member of staff or a parent. As examples, staff can also be parents (of pupils at the school), in relationships or have friendships with other staff or parents; or also governors. Any member of staff can report any social media relationships to senior leaders for their own protection.
* Staff must make sure that their personal social media activities take into account who they have social media relationships with – particularly any other members of school community – and moderate their social media behaviour accordingly.
* Personal use of social media at school:
* School staff can make reasonable personal use of social media during the working day or while at their school. This must not interfere with any work activities.
* Staff can only use social media when no pupils are present and during breaks or non-directed time.
* Staff can use school devices where social media sites can be accessed using school systems. This use must also follow the school’s staff acceptable use policy (AUP).
* There is no obligation on the school to make social media sites available to staff.
* Staff can only use personal devices with social media while at their school where the use of personal devices is allowed by the school. Again, this use must still follow the school’s acceptable use policy (AUP).

**9 Excessive use of social media at school**

* Staff must not spend an excessive amount of time while at the school on personal use of social media. They must ensure that use of social media does not interfere with their duties.

**10 Monitoring use of social media on school equipment**

* The school reserves the right to monitor all staff internet use, including when staff are making personal use of social media, on any school systems or equipment. Misuse of social media – even personal use – on school equipment is a breach of the school’s acceptable use policy.

**11 Disciplinary action over social media use**

* All staff are required to adhere to this policy. Staff should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the school, may constitute gross misconduct and lead to summary dismissal.
* Similarly, where there is a serious breach of this policy, action may be taken in respect of other members of staff who are not employees (volunteers) which may result in the termination of their appointment.

**12 If you have any concerns**

* When using social media, you may have a concern about what you are seeing or being told by another user which has safeguarding implications or may cause harm to the reputation of the school and/or its community. If you have any such concerns you should contact the head teacher, the named safeguarding contact in school, or human resources for advice.
* If a member of staff becomes aware that a pupil (or group of pupils) or parent has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they should consider reporting this to the head teacher so that the appropriate process can be followed, and support can be offered to the employee.

APPENDIX 5

**Digital Permission Form**

APPENDIX 6

**Seesaw Permission Form**