**GNFC Online Safety Policy**

**Feb 2021**  **To be reviewed Feb 2022**

Development / Monitoring / Review of this Policy was done in consultation with the following:

* Senior Leaders
* Online Safety Coordinator
* Staff
* Parents and Carers
* DSL

**Schedule for Development / Monitoring / Review**

|  |  |
| --- | --- |
| This Online Safety policy was approved by Senior Leaders: |  |
| The implementation of this Online Safety policy will be monitored by the: | *Senior Leadership Team,* |
| Monitoring will take place at regular intervals: | *Yearly* |
| The Directors will receive a report on anonymous details of online safety incidents at regular intervals: | *Yearly* |
| 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: | *10/02/22* |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | *LADO, Police* |

GNFC will monitor the impact of the policy using:

* Logs of reported incidents
* Monitoring logs of internet activity
* Internal monitoring data for network activity
* Surveys / questionnaires of
  + children
  + parents / carers
  + staff
  + residents

**Scope of the Policy**

This policy applies to all members of ourcommunity (including staff, residents, volunteers, parents / carers, visitors, community users) who have access to and are users of GNFC digital technology systems, both in and out of our sites.

Leaders will take action to such extent as is reasonable, for inappropriate behaviour online. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of our sites , but is linked to membership of the organisation. Action can only be taken over issues covered by the published Behaviour Policy.

GNFC will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where appropriate, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place off site.

## **Roles and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals and groups within GNFC:

**Senior Leaders**

Senior Leadersare responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Leaders receiving regular information about online safety incidents and monitoring reports. A member of the Leadership Team has taken on the role of Online Safety Co-ordinator. Thiswill include:

* attendance at Online Safety Group meetings
* regular monitoring of online safety incident logs
* regular monitoring of filtering / change control logs
* reporting to relevant Governors
* Managers have a duty of care for ensuring the safety (including online safety) of members of the GNFC community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
* Managers 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 / MAT / other relevant body disciplinary procedures).
* Managers are responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* Managers will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

**Online Safety Co-ordinator**

* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policy / 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 / MAT / relevant body as appropriate
* liaises with technical staff
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
* Reports to Directors to discuss current issues, review incident logs and filtering / change control logs
* reports regularly to Senior Leadership Team

**Technical staff**

The Technical Staff are responsible for ensuring:

* that the technical infrastructure is secure and is not open to misuse or malicious attack
* that GNFC meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy.
* A filtering system, is applied and updated on a regular basis.
* 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 Directors; for investigation / action / sanction
* that monitoring software / systems are implemented and updated

Other Staff are responsible for ensuring that:

* they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices
* they have read, understood and signed other relevant policies eg Social Media Policy
* they report any suspected misuse or problem to Managers for investigation / action / sanction
* all digital communications with residents / children / parents / carers should be on a professional level *and only carried out using official systems*
* online safety issues are embedded in all aspects of the activities of GNFC
* Residents and children understand and follow the Online Safety Policy
* they monitor the use of digital technologies, mobile devices, cameras etc during the working day (where allowed) and implement current policies with regard to these devices
* *in lessons where internet use is pre-planned children 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
* online-bullying

**Residents and children:**

* are responsible for using the school digital technology systems in accordance with this policy
* 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 online-bullying.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. GNFC will take every opportunity to help parents understand these issues through discussion as appropriate *.* Parents and carers will be encouraged to support GNFC in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at events
* their children’s personal devices on our sites

**Community Users**

Community Users who access our systems as part of our outreach programme will be expected to abide by all relevant policies.

# **Policy Statements**

**Education**

Whilst regulation and technical solutions are very important, their use must be balanced by educating residents and children to take a responsible approach. The education in online safety / digital literacy is therefore an essential part of GNFC’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 and staff should reinforce online safety messages. In addition it is important to ensure the following:

* Key online safety messages should be reinforced as part of a planned programme of activities
* Children should be supported in building resilience to radicalisation by providing a safe environment for talking about similarities and differences, rules and reasons for them and encouraging mutual respect and acceptance.
* Staff should act as good role models in their use of digital technologies, the internet and mobile devices

In situations where internet use is pre-planned, it is best practice that sites are checked as suitable for use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

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.

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

* *Letters, newsletters, web site*
* *Information sessions during regular meetings*
* *Reference to the relevant web sites / publications e.g.*

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:

* Formal online safety training will be made available to nursery 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 nursery staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Online Safety Policy.
* It is expected that some staff will identify online safety as a training need within the performance management process.
* This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.

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

The GNFC will be responsible for ensuring that the 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 will be effective in carrying out their online safety responsibilities:

* Technical systems will be managed in ways that ensure that GNFC meets recommended technical requirements
* There will be regular reviews and audits of the safety and security of technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to technical systems and devices.
* All users will be provided with a username and secure password .
* Internet access is filtered for all users. Illegal content (eg child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
* Internet filtering / monitoring should ensure that children and residents are safe from terrorist and extremist material when accessing the internet**.**
* An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
* Appropriate security measures are in place to protect the firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the systems and data. These are tested regularly. The infrastructure and individual workstations are protected by up to date virus software.
* Personal data cannot be sent over the internet or taken off the site unless safely encrypted or otherwise secured*.*

**The charity allows:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | GNFC Devices | | | Personal Devices | |
|  | **GNFC owned for single user** | **GNFC owned for multiple users** | **Authorised device**[[1]](#footnote-1) | **Resident/child owned** | **Staff owned** |
| Allowed on site | *Yes* | *Yes* | *Yes* | To be kept in office in nursery if belonging to a nursery child. | To be kept out of sight (in bags) in nursery if belonging to nursery staff or other staff in nursery eg Jo |
| Full network access | *Yes* | *Yes* | *Yes* |  |  |
| Internet only |  |  |  |  |  |
| No network access |  |  |  |  |  |

**Use of digital and video images**

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

When using digital images, staff should inform and educate residents/children 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 children are published on the 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 events for their own personal use (as such use is 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 children in the digital / video images.
* Staff and volunteers are allowed to take digital / video images to support aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be taken on GNFC equipment, the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or GNFC into disrepute.
* Residents/Children must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
* Residents/Childrens full names will not be used anywhere on a website or blog, particularly in association with photographs.

**Dealing with unsuitable / inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from GNFC and all technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in the context of GNFC, either because of the age of the users or the nature of those activities.



**Other Incidents**

It is hoped that all members of the GNFC community will be responsible users of digital technologies, who understand and follow this 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 involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Where possible conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  + Internal response or discipline procedures
  + Involvement by Local Authority / local organisation (as relevant).
  + Police involvement and/or action
* **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  + incidents of ‘grooming’ behaviour
  + the sending of obscene materials to a child
  + adult material which potentially breaches the Obscene Publications Act
  + criminally racist material
  + promotion of terrorism or extremism
  + 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 (possibly for the police) and demonstrate that visits to these sites were carried out for safeguarding purposes. All notes should be retained by the group for evidence and reference purposes.

**Actions & Sanctions**

It is more likely that GNFC will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the GNFC community are aware that incidents have been dealt with.

[Introduction 4](#__RefHeading__13159_668335512)

[[Name of School / Academy]  
Online Safety Policy 7](#__RefHeading__13161_668335512)

[Policy Statements 13](#__RefHeading__13191_668335512)

[Appendices 49](#__RefHeading__13227_668335512)

[Student / Pupil Acceptable Use Agreement Template – for older students / pupils 49](#__RefHeading__13229_668335512)

[Student / Pupil Acceptable Use Agreement Form 53](#__RefHeading__13231_668335512)

[Student / Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1) 54](#__RefHeading__13233_668335512)

[Parent / Carer Acceptable Use Agreement Template 54](#__RefHeading__13235_668335512)

[Staff (and Volunteer) Acceptable Use Policy Agreement Template 58](#__RefHeading__13237_668335512)

[Acceptable Use Agreement for Community Users Template 62](#__RefHeading__13239_668335512)

[Responding to incidents of misuse – flow chart 63](#__RefHeading__13241_668335512)

[Record of reviewing devices / internet sites (responding to incidents of misuse) 64](#__RefHeading__13243_668335512)

[Reporting Log 65](#__RefHeading__13245_668335512)

[Training Needs Audit Log 66](#__RefHeading__13247_668335512)

[School Technical Security Policy Template (including filtering and passwords) 67](#__RefHeading__13249_668335512)

[School / Academy Personal Data Advice and Guidance 74](#__RefHeading__13259_668335512)

[School / Academy Policy Template: Electronic Devices - Searching & Deletion 83](#__RefHeading__13261_668335512)

[Mobile Technologies Policy Template (inc. BYOD/BYOT) 88](#__RefHeading__13263_668335512)

[Social Media Policy Template 92](#__RefHeading__13269_668335512)

[School Policy Template – Online Safety Group Terms of Reference 97](#__RefHeading__13277_668335512)

[Legislation 99](#__RefHeading__13279_668335512)

[Links to other organisations or documents 103](#__RefHeading__13281_668335512)

[Glossary of Terms 106](#__RefHeading__13283_668335512)

1. [↑](#footnote-ref-1)