# *Online Safety Policy*

| | |
|---|---|
| **Person Responsible:** | G. Rughoobeer (Head of Compliance/DSL), ratified by B. Elkins (Headteacher) |
| **Last reviewed on:** | August 2024 |
| **Next review due by:** | August 2025 |
| **Created:** | February 2022 |
| **Revisions:** | August 2023, August 2024 |

*Gretton School is owned and operated by Newcome Education, a subsidiary group of Cavendish Education.*

*This policy is one of a series of school policies that, taken together, are designed to form a comprehensive statement of the school's aspiration to provide an outstanding education for each and every one of its students and of the mechanisms and procedures in place to achieve this. Accordingly, this policy should be read alongside all of these policies in order to ensure an awareness of the bigger picture. In particular it should be read in conjunction with the Equality Policy, the Health and Safety Policy and the Safeguarding Children and Child Protection Policy.*

*All of these policies have been written, not simply to meet statutory and other requirements, but to evidence the work that the whole school is undertaking to ensure the implementation of its core values.*

*In all the school's policies, unless the specific context requires otherwise, the word "parent" is used in terms of  Section 576 of the Education Act 1996, which states that a 'parent', in relation to a child or young person, includes any person who is not a parent (from which can be inferred 'biological parent') but who has parental responsibility*
*, or who has care of the child. [Department for Education guidance](#) considers a 'parent' to include:*
- *all biological parents, whether they are married or not*
- *any person who, although not a biological parent, has parental responsibility for a child or young person - this could be an adoptive parent, a step-parent, guardian or other relative*
- *any person who, although not a biological parent and does not have parental responsibility, has care of a child or young person*

*A person typically has care of a child or young person if they are the person with whom the child lives, either full or part time and who looks after the child, irrespective of what their biological or legal relationship is with the child.*

*The school employs the services of the following consulting companies to ensure regulatory compliance and the implementation of best practice:*
- *Peninsula HROnline*
- *Peninsula BusinessSafe (Health and Safety)*
- *Carecheck (DBS)*
- *Educare (online CPD)*

# Online Safety Policy

GRETTON SCHOOL

## CONTENTS

## 1 SCOPE

This policy applies to all members of the school community (including staff, learners, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's digital technology systems, both in and out of the school.

This policy seeks to support all stakeholders to manage their use of technology in line with the school's Positive Relationships Policy, i.e. with respect, consideration of others, safely and with a mind to the reputation of the school and its ethos.

GRETTON SCHOOL

When learners or staff are using social media platforms or other means of communication with others within the school community, the school expects that they will do so in a way that maintains respectful boundaries, uses supportive and respectful language and would not be perceived to be bullying others.

The school will deal with such incidents outlined within this policy and associated Positive Relationship (Behaviour) Policy and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that may take place both within and outside of school. It may then be necessary for school and families to work together to address the issues raised in order to resume a more appropriate use of technology and address any bullying or inappropriate conduct.

## 2 ROLES AND RESPONSIBILITIES

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

### 2.1 Governors/Board of Directors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:
- Regular meetings with the nominated staff member for Online Safety
- Attendance at Online Safety Group meetings
- Regular monitoring of Online Safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors/Board/Committee/meeting

### 2.2 Headteacher and Senior Leaders

Headteacher and School Leadership Team is responsible for ensuring:
- The safety (including online safety) of members of the school community, although the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- That they are 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 – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures)
- That the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- That there is a system in place to allow for monitoring of online safety issues or concerns
- That they review any online safety issues or concerns as part of their ongoing monitoring of school data.

## 2.3 The Online Safety Lead

The Online Safety Lead will:
- Lead or support the Online Safety Group
- Take day to day responsibility for online safety issues and concerns and play a leading role in establishing and reviewing the school's online safety policies/documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority/Proprietary Body
- Liaise with school technical staff
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attend relevant meetings of Governors, where required
- Report regularly to School Leadership Team

## 2.4 Network/IT Manager

The Network/ICT Manager will:
- Ensure that school's technical infrastructure is secure and is not open to misuse or malicious attack
- Meet required online safety technical requirements and any Local Authority/relevant body online safety policy/guidance that may apply
- Ensure that users may only access the networks and devices through a properly enforced password protection policy
- Ensure that the filtering policy is applied and updated on a regular basis
- Ensure 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
- Ensure that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders or the Online Safety Lead for investigation/ action/sanction
- Ensure that monitoring software/systems are implemented and updated as agreed in school policies

## 2.5 Teaching and Support Staff

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 and use the Devices Charter in the classroom.
- They report any suspected misuse or problem to the Online Safety Lead/Safeguarding Team and on My Concern for investigation or action

GRETTON SCHOOL

- All digital communications with learners/parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded across the curriculum and other activities
- Learners understand and follow the principles of the school's Online Safety approach and have seen and agreed to the acceptable use policies
- Learners understanding the basics of research skills and the need to avoid plagiarism
- They monitor the use of digital technologies, personal devices, cameras, etc. if used in line with the Devices Charter in class and/or other school activities (where permitted use) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, learners are 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

## 2.6 Designated Safeguard Lead/Designated Persons

DSL, DDSLs and DPs 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

All of the above concerns should be reported, recorded and responded in the usual way in terms of safeguarding matters, using MyConcern and raising issues to appropriate external bodies where required.

## 2.7 Learners

It is the responsibility of learners to:
- Make use of the school digital technology systems in accordance with the learner acceptable use agreement
- Avoid plagiarism
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Ensure that the use of personal devices and digital cameras follows the acceptable use agreement
- Engage in learning about online safety and learn measures to keep themselves and others safe online, including the taking/using of images and online-bullying
- Understand the importance of adopting good online safety practice when using digital technologies out of school and recognise that the school's online safety policy covers their actions out of school, if related to their membership of the school
- Recognise that their own use of social media and online communication platforms can on occasion have a negative impact on other learners within the school and that in these cases, the school may take steps to communicate with their parents to address this behaviour

GRETTON SCHOOL

## 2.8 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/personal devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, website, social media 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 from the parents' sections of the website and NOS Learning Platform in order to ensure the appropriate use of:
- Digital and video images taken at school events
- Their children's personal devices in the school
- Their children's use of social media and online communication platforms

## 3  POLICY STATEMENTS

## 3.1 Education - Learners

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

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:
- A planned online safety curriculum is provided as part of Computing/RSE/ PSHE/other lessons and is regularly revisited.  This includes 4 mains areas, as follows:
  - Content - fake news and harmful content
  - Conduct - online behaviour including child-on-child abuse
  - Contact - harmful interactions online, including gaming
  - Commerce - risks of phishing, scamming, financial scams and gambling
- Some aspects of the curriculum above are also covered in the English secondary curriculum.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Learners will 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
- Learners will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners will 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

- Learners will be helped to understand the need for the learner/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy
- Staff will act as good role models in their use of digital technologies, the internet and personal devices
- In lessons where internet use is pre-planned, it is best practice that learners are 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 learners are allowed to freely search the internet, staff must 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, learners 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 Network/IT Manager 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

## 3.2 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 online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, NOS Learning Platform
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications
- Working with external partners to promote learning and understanding

## 3.3 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/academy 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 Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

GRETTON SCHOOL

- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions
- The Online Safety Lead (will provide advice/guidance/training to individuals as required

## 3.4 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 other relevant organisations
- Participation in school training/information sessions for staff or parents

## 4 TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school 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:
- School technical systems are managed in ways that ensures the school meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school/academy technical systems
- Servers, wireless systems and cabling are securely located and physical access 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 the Network/IT Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "master/administrator" passwords for the school systems, used by the Network/IT Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The Network/IT Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations where applicable
- Internet access is filtered for all users. Illegal content (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 are safe from terrorist and extremist material when accessing the internet.
- School Network/IT Manager regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement

- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, personal devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual 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
- An agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

## 5 PERSONAL TECHNOLOGIES/DEVICES

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

All users are required to confirm their understanding that the primary purpose of the use of personal/personal devices in a school context is educational. Staff processes for this are detailed in the Staff Handbook and form part of the induction process within school. The personal technologies policy is consistent with and interrelated to other relevant school policies including but not limited to the safeguarding policy, positive relationships (behaviour) policy, bullying policy and acceptable use policy. Teaching about the safe and appropriate use of personal technologies is an integral part of the school's online safety education programme. Visitors will be informed about school requirements regarding online safety and the use of personal phones whilst on site via the distribution of the Gretton School Visitor Information Leaflet.

## 6 USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may

provide avenues for online-bullying to take place and other more serious incidents. 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. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- Written permission from parents/carers will be obtained before photographs of learners 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 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 *learners* in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims using school devices only, and must follow school policies concerning the sharing, distribution and publication of those images. The personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Learner's work can only be published with the permission of the learner/pupil and parents or carers

## 7 DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
As a school we ensure that:

- We have a Data Protection Policy
- We implement data protection principles through policy and everyday practice
- We have paid the appropriate fee for Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO)
- We have appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest

# *Online Safety Policy*

- We have an 'information asset register' in place and know exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The 'information asset register' records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- We will hold only the minimum personal data necessary to enable it to perform its function and we will not hold it for longer than necessary for the purposes it was collected for.  The school has and implements a retention policy to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held is accurate and up to date where this is necessary for the purpose it is processed for. We have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- We provide staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access Request which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply)
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- We have undertaken appropriate due diligence and have applied data processing clauses in contracts with any data processors where personal data is processed
- We understand how to share data lawfully and safely with other relevant data controllers
- We report any relevant breaches to the Information Commissioner within 72 hrs of becoming aware of the breach, in accordance with UK data protection law. We also report relevant breaches to the individuals affected as required by law. In order to do this,we have a policy for reporting, logging, managing, investigating and learning from information risk incidents
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

**When Personal data is stored on any personal device or removable media for any reason, the:**
- Data must be encrypted and password protected
- Device must be password protected
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with the schools policy once it has been transferred or its use is completed

# Online Safety Policy

**Staff must ensure that they:**
- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written, and know who to pass it to in school
- Where personal data is stored or transferred on personal or other devices (including USBs) these must be encrypted and password protected
- Will not transfer any school/academy personal data to personal devices
- 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

## 8 COMMUNICATIONS

A wide range of communication technologies are available and these can enhance learning when used correctly. The following table shows how as a school we currently consider the benefit of using these technologies for education measured against any possible risks or disadvantages:

| Communication Technologies | Staff & other Adults | | | Learners | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| | Allowed | Allowed in designated areas | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not Allowed |
| Personal devices (dumb phones only) brought to school | | ✅ | | | ✅ | ✅ | |
| Use of personal devices in lessons | | | ✅ | | | | ✅ |
| Use of personal devices in social time | | ✅ | | | ✅ | ✅ | |
| Taking photos on personal devices or personal camera device | | | ✅ | | | | ✅ |
| Use of other personal devices e.g. tablets, gaming devices | | ✅ | | | | | ✅ |
| Use of personal email addresses in school, or on | | | ✅ | | | | ✅ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| school network during own time | | | | | | | | |
| Use of school email for personal emails | | | ✅ | | | | | ✅ |
| Use of chat rooms/facilities | | | ✅ | | | | | ✅ |
| Use of messaging apps | | ✅ | | | | | | ✅ |
| Use of social network sites | | ✅ | | | | | | ✅ |
| Use of personal blogs | | | ✅ | | | | | ✅ |
| Use of educational blogs | ✅ | | | | | ✅ | | |

**Please note the school is a Residential Special School so learners would use their personal equipment outside of school hours with support and guidance from residential staff.**

---

When using communication technologies, the school considers the following as good practice:
- The official school email service is regarded as safe and secure and is monitored. Users are aware that email communications are monitored
- Users are supported to understand that they 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 learners or parents/carers (email, social media, chat, blogs, VLE etc) is professional in tone and content and only via a school email address/personal device
- Learners are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and regularly reminded of the need to communicate appropriately when using digital technologies
- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff

---

## 9 SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party, may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, 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 are in place
- Risk assessments, including legal risk are used where necessary

**School staff are aware that:**
- No reference should be made on social media platforms to learners, parents/carers or the school/school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

**Where official school social media accounts are established there is:**
- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- Protocols of behaviour for users of the accounts are in place, including processes for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

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

**Monitoring of Public Social Media:**
- As part of active social media engagement, we will proactively monitor the internet for public postings about the school
- The school will not respond to social media comments made by others that are of a negative nature and which may bring the school's reputation into disrepute
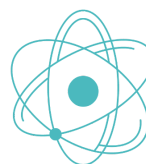
The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

## 10 DEALING WITH UNSUITABLE/INAPPROPRIATE ACTIVITIES

# *Online Safety Policy*

GRETTON
SCHOOL

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and access to such platforms is prohibited across all technical systems. Any other activities determined to be unacceptable, e.g. cyber-bullying will be addressed through our policies and may lead to criminal prosecution. We acknowledge that there may be a range of activities that may be legal but would nevertheless be inappropriate in a school context, either because of the age of the users or the nature of those activities.
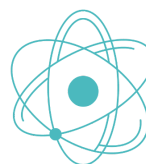
For clarity, the school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems and may be referred to statutory services.

| The school policy restricts usage as follows: | | | | | |
| --- | --- | --- | --- | --- | --- |
| **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 that are 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 or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008 | | | | | ✅ |
| Criminally racist material in the UK – to incite 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 the school or brings the school into disrepute | | | | ✅ | |
| Activities that might be classed as cyber-crime under the Computer Misuse Act:<br>● Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>● Creating or propagating computer viruses or other harmful files<br>● Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, | | | | | ✅ |

| | | | | | |
|---|---|---|---|---|---|
| computer / network access codes and passwords)<br>● Disable/Impair/Disrupt network functionality through the use of computers/devices<br>● Using penetration testing equipment (without relevant permission) | | | | | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | ✅ | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | | | | ✅ | |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | ✅ | |
| Using school systems to run a private business | | | | ✅ | |
| Infringing copyright | | | | ✅ | |
| Online gaming (educational) by agreement | ✅ | | | | |
| Online gaming (non-educational) | | | ✅ | | |
| Online gambling | | | | ✅ | |

| | | | | | |
|---|---|---|---|---|---|
| Online shopping/commerce | | | ✅ | | |
| File sharing | | | ✅ | | |
| Use of social media | | | ✅ | | |
| Use of messaging apps | | | ✅ | | |
| Use of video broadcasting e.g. Youtube | | | ✅ | | |
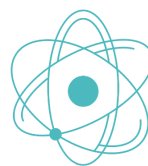
## 11 RESPONDING TO INCIDENTS OF MISUSE

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

## 11.1 Illegal Incidents

Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

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

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

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.

Illegal materials or activities found or suspected

This will only be done by a DSL.

Report to Police using any number and report under local safeguarding arrangements.

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

Secure and preserve evidence.

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

Call professional strategy meeting

Await Police response

If no illegal activity or material 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

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

## 11.2 Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported and will be directed by the DSL
- 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)
- Once this has been completed and fully investigated the group will need to judge whether this concern is to be upheld 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 Newcome and/or the Cavendish group
  - 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. Under no circumstances should the images be looked at, downloaded or sent onward in the case of potentially illegal images. 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 Offenses under the Computer Misuse Act (see User Actions chart above)
- o Other criminal conduct, activity or materials

The Online Safety Lead will isolate the computer in question to protect an evidence trail for the school and possibly the police, demonstrating 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 and where.

## 11.3 School Actions

It is more likely that the school 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 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 identified in the schools Positive Relationships (Behaviour) Policy.

Specific learner incidents could be (but are not limited to):
- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised/inappropriate use of personal phone/digital camera/other personal 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 learner's/pupil'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/academy into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's 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

## 11.4 Staff Incidents (examples of, not limited to)

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).
- Inappropriate personal use of the internet/social media/personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules

- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with learners
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

The above and any other relevant incident could result in the following:
- Referral to line manager
- Referral to the headteacher
- Referral to HR resulting in disciplinary action in line with the schools disciplinary policy
- Referral to the police

## 12 ONLINE SAFETY IN THE BOARDING PROVISION

### 12.1 Communications

**12.1a Personal devices**
Learners are permitted to use personal personal phones within the residential provision, subject to risk assessment where necessary and agreement by parents, carers or other responsible adults (e.g. social workers)

**12.1b Social networking websites and apps**
Social networking sites have undoubted benefits but also pose risks to learners e.g. online bullying, radicalisation and the risk of adults disguising their identity in an attempt to mislead minors. In safeguarding and promoting the welfare of each learner, their access to social networking websites and apps at Gretton will be managed as followed:
- Written consent will be sought from parents, carers or other responsible adults (e.g. social worker). Where consent is not given, details will be recorded in the learner's relevant plan(s) and risk assessment and access will not be granted
- Where written consent is provided, we will include in the learner's risk assessment
- Where the risk of harm is calculated to be 'high' or 'very high', we are committed to working with parents, carers, local authority representatives and the learner, in order to establish a way forward in promoting their access to social media
- Irrespective of consent or risk assessment, we will not permit learner's access to social networking websites or apps, if they fail to meet the minimum age criteria

## 12.2 Equipment and storage PCs, laptops, tablets, Personal Digital Assistants (PDAs) and USB pen drives

The possession and use of personal computers, laptops, tablets and PDAs must be agreed on admission by parents, carers or other responsible adults (e.g. social workers) and will be collected by school staff upon arrival. Items will be bagged and locked in storage until collection at the end of the school day, unless there is pre-agreed independent travel or in the event of a school trip where permissions have been sought.. Given the high storage capacity of PCs, laptops, tablets, PDAs and USB pen drives it is not logistically possible to undertake the frequency of checks necessary to ensure the suitability of all files. However, all devices with storage capability must be made available to staff, as and when required, for the purpose of monitoring content. Gretton does not accept responsibility for any loss or damage to any PCs, laptops, tablets, Personal Digital Assistants (PDAs) and USB pen drives, unless placed in the care of our staff.

## 12.3 Entertainment

### 12.3a MP3 and MP4 players
While an 'MP3 player' can be used to store, organise and play audio files only, an 'MP4 player' can also be used to play audio files and view text files, images and videos. While such devices are considered acceptable, staff should be aware of the high storage capacity of some models. All devices with storage capability must be made available to staff, as and when required, for the purpose of monitoring content. Gretton does not accept responsibility for any loss or damage to any MP3 or MP4 player, unless placed in the care of our staff.

### 12.3b Games consoles and hand-held devices e.g. Nintendo 3DS
The possession and use of games consoles and other hand-held devices is considered acceptable for transport to and from school. However, these should be handed in upon arrival. Learners with devices that have internet capacity and storage capability of the current generation of games consoles and hand-held devices will not be able to use these during the school day. Staff will monitor the suitability and age appropriateness of games. All devices with storage capability must be made available to staff, as and when required, for the purpose of monitoring content. Gretton does not accept responsibility for any loss or damage to any games console or handheld device, unless placed in the care of our staff.

### 12.3c Films and DVD's
Staff need to ensure the suitability of these when learners are watching them.

GRETTON SCHOOL