ROYSTON SCHOOLS ACADEMY TRUST

The Greneway School

eSafety Policy

Reviewed by:	Curriculum and Achievement	June 2017
Ratified by:	Full Governors	July 2017
Next Review:		June 2019 *
Statutory Document:	N	
Update on Website:	Y/N	
Additional Comments:	There will be on-going opportunities for staff to discuss with the ITC 4 Learning Group any issue of eSafety that concerns them. This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning. *The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.	

Contents:

The Greneway School eSafety Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

At Greneway, we feel it is essential to provide pupils with a clear understanding of how to use technology safely both in school and in the wider world. Currently, the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- APPs
- Google Drive and Virtual Learning Environments
- Email, Instant Messaging and chat rooms
- Social Networking, including Facebook and Twitter
- Mobile/Smart phones with text, video and/or Internet access
- Other mobile devices including tablets and gaming devices
- Online games
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 .

At Greneway, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, ChromeBooks, laptops, iPads, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The ITC 4 Learning Group at Greneway has been designated the role to oversee eSafety. All members of the school community have been made aware of members of the group. It is the role of the ITC 4 Learning Group to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child

Exploitation and Online Protection) and Childnet. A designated member of the group has been allocated responsibility for keeping the rest of the group up to date on eSafety matters (JG).

Senior Management and Governors are updated by the Head/ ICT 4 Learning Group and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (Appendix 1), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE**.**

eSafety skills development for staff

- Staff receive regular information and training on eSafety issues in the form of staff communications, INSET, assemblies and attendance on updated training.
- Details of the ongoing staff training log can be found by contacting the deputy head who has a responsibility for CPD.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see Appendix 2)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas. Staff are regularly provided with materials to support eSafety across the curriculum and informed with up-to-date areas of concern.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the Internet and/or related technologies are used.
- The eSafety AUP is introduced to the pupils at the start of each school year. Pupils have to review and resign the schools AU Agreement. Reminders of key messages are regularly displayed for pupils to review.
- E-safety posters are prominently displayed.
- Key, up-to-date eSafety advice is promoted with pupils in school and with parents through the school blog and Twitter.
- Greneway participates in Safer Internet Day every February.
- Pupils can report eSafety issues to the ITC 4 Learning Team via the email address on the website: reportproblems@greneway.herts.sch.uk

eSafety in the Curriculum

ICT and online devices are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching Internet skills in ITC/ PSHE lessons
  (See ITC overview/Included on PSHEE 'Safety' Day for all pupils every year)
- The school provides opportunities within a range of curriculum areas to teach about eSafety. (See Greneway School eSafety Overview)
- Educating pupils about the online risks they may encounter outside school is covered informally when opportunities arise **and** as part of the eSafety curriculum.
- Pupils are made aware of the relevant legislation when using the Internet such as data protection and intellectual property rights which may limit what they want to do but also serves to protect them.

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button. School assemblies draw attention to this issue.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ITC curriculum *(see ITC overview)*

Passwords
General advice - see staff reminders sheet (Appendix 4)

Password Security
Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security. All pupil passwords are reset at the start of the school year.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy. A termly reminder of key points to remember is provided when logging on to the network.
- Users are provided with an individual network, email and Google Drive log-in username (as appropriate).
- If it becomes clear that a password may have been compromised or someone else has become aware of a password, it should be reported to the Network Manager
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS and/or Google Drive, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that laptops/ChromeBooks and iPads are not left unattended and are locked.
- Due consideration should be given when logging into Google Drive to the browser/cache options (shared or private computer)
- At Greneway, all ITC password policies are the responsibility of the Network Manager and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT
- Staff are aware of their responsibility when accessing school data.
- Staff have access to relevant guidance documents re safe handling of data.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential and classified data.

- Staff should avoid leaving any portable or mobile devices or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry any portable or mobile devices or removable storage media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any sensitive, confidential and classified information contained in documents faxed, copied, scanned, printed or share via Google Drive.
- Anyone sending a confidential or sensitive fax should notify the recipient before hand.

Managing the Internet

The Internet is an open worldwide communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **HICS** (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet connectivity.
- Staff will preview any recommended sites, online services, software and APPs before use. RMTutor allows teaching staff to limit the Internet sites used within a lesson.
- Specific key search terms are encouraged when pupils are searching for images.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Names of colleagues, pupils, others or any other confidential information acquired through the job must NOT be revealed on any social networking site or other online application.
- Online gambling or gaming is not allowed.

It is at the head teacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the HICS where web-based activity is monitored and recorded.
- School internet access is controlled through the HICS web filtering service.
- The Greneway School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Network Manager and ITC 4 Learning Group.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Antivirus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the network manager's, to install or maintain virus protection on personal systems. Pupils are encouraged to create and/or access their school work via Google Drive. If they wish to bring in work on removable media, it must be given to the technical support team for a safety check first.
- Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from Network Manager.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed (*via Google Sites Technical Support*).

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking (with the exclusion of Twitter) and online gaming sites to pupils within school.
- All pupils and staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils and staff are taught/advised to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils and staff are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Pupils and staff are advised to set and maintain their online profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils and staff are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Pupils and staff are asked to report any eSafety incidents (Pupils - via the website reportproblems@greneway.herts.sch.uk / Staff via the eSafety log accessed on Greneway Dashboard, Google Drive)
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using Google Sites or other systems approved by the Headteacher.
- When using the school's Twitter Accounts, staff are reminded to stay anonymous as far as possible and ensure all communication is appropriate. Naming individual pupils, alongside an image, on Twitter is to be avoided.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, iPads/tablets, gaming devices, mobile and Smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under exceptional circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device (for example, during a school journey). The Headteacher should be notified of this use.
- Pupils are allowed to bring personal mobile devices/phones to school but are required to leave them in the school office from the beginning of the school day. In line with practices at the upper school, year 7 and 8 pupils are expected to keep these devices, turned off, in their personal locker - alternatively, it may be handed into the office for safekeeping. Pupils in Yrs 5 & 6 must hand in switched off phones to the office for safekeeping.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
    - See staff agreement signed by all staff using school provided mobile devices for staff responsibility linked to the device.

Portable and Mobile ICT Equipment

This section covers such items as laptops, chromebooks, mobile devices and removable data storage devices. This should be read in conjunction with the section of this document referring to storing and transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network/Google Drive and not kept solely on the hard drive of a device. Any equipment where personal data is likely to be stored should be encrypted.
- Equipment must be physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, equipment should be placed in the boot of the cr before starting the journey.
- Ensure portable devices and mobile technology equipment is available as necessary for anti virus updates and software installations or upgrades.

- The installation of any applications or software packages must be authorised by the Network manager, fully licensed and carried out by an ICT Technician.
- or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsibly online'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. This ensures the traceability of all emails through the school system.
- Staff and governors should use their school email address for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- The school attaches a standard disclaimer to all email correspondence sent out of the RSAT community. It states that views expressed are not necessarily those of the school or the LA.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed notepaper.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Therefore, it is expected that staff actively manage their email account by a) deleting all emails of short term value and b) organise emails into appropriate folders and carry out frequent housekeeping on all folders and archives.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- All pupils have their own individual school issued accounts which are introduced as part of the ITC curriculum (This is reviewed yearly with all year groups). Pupils may only use their school email accounts on the school system.
- The forwarding of chain letters is not permitted in school. Pupils may forward chain emails to: reportproblems@greneway.herts.sch.uk
- All email users are expected to adhere to the generally accepted rules of accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. This email could be forwarded to: reportproblems@greneway.herts.sch.uk
- Staff must inform (the ITC 4 Learning Group) if they receive an offensive e-mail.
- However staff/pupils access their email account (in school or on non school hardware) all the school email policies apply.

Sending emails

- When sending emails, staff are expected to use their school email address so that they can be clearly identified as the originator of a message.
- Staff are expected to keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.

Receiving emails

All staff are expected to:

- Check email regularly.
- Activate an out of office notification when away for extended periods.
- Never open attachments from an untrusted source.
- Do not use email systems to store attachments. They should be downloaded and saved in appropriate shared drives/folders.

eMailing Personal, Sensitive, Confidential or Classified Information

Where the conclusion is that email must be used to transmit data:
EITHER: Use Schools Fx, Herts Fx or Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely.
http://www.thegrid.org.uk/eservices/schoolsfx.shtml
OR:

- Obtain express permission from line manager and/or Head Teacher to provide the information by email.
- Verify the details, including accurate email address, of any intended recipient.
- Verify (by phoning) the details of the requestor BEFORE responding to email requests for information. Do not send information to any person whose details it has been unable to verify.
- Send the information as an encrypted and password protected document **attached** to an email. See: http://www.thegrid.org.uk/info/dataprotection/#securedata
- Send the encryption key or password by a **separate** contact with the recipient.
- DO NOT copy or forward the email to any more recipients than is absolutely necessary.
- Do not include any identification information in the subject line of the email.
- Request confirmation of safe receipt.

Social Media, *including Facebook and Twitter*

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our lives.

- Greneway School uses Twitter to communicate with staff, pupils, parents, carers and the wider community. Staff (appropriate to the subject area) are responsible for all postings on these technologies and monitoring responses in line with the school's AUP.
- Staff are not permitted to access their personal social media accounts using school equipment during school hours.
- Staff are able to set up social media accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of social media.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are made aware that the information, comments, images and videos they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are made aware that their online behaviour should at all times be compatible with UK law.

In case of inappropriate behaviour on Twitter, the following procedures will be implemented: User Blocked; Account made private (Tweets protected); Account Terminated.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others in school. However with the express permission of the Headteacher, images can be taken on school field trips provided they are for educational purposes.
- Pupils and staff must have the permission from the head teacher before any image can be uploaded for publication.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Google Sites / Blogs / Twitter
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Designer/Admin. Team has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network or on Google Drive.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Google Drive/Sites/Blogs.
- The Network Manager has the responsibility of archiving the images when they are no longer required.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the School and Premises Managers. Notification of CCTV use is displayed at the front of the school. The school has a CCTV policy which is reviewed annually.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Webcams will not be used for broadcast on the Internet without prior parental consent.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document).
- Webcams include any camera on an electronic device which is capable of producing video footage.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- ➢ Participants in conferences offered by 3rd party organisations may not be DBS checked.
- ➢ Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

It is the responsibility of staff to ensure that:

- any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended
- you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multifunction print, fax, scan and copiers) are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the Internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean
- For further guidance on How to Encrypt Files
  - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Remote Access

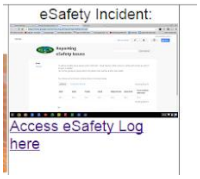
- You are responsible for all activity via your remote access facility (EG Sensitive data accessed via Google Drive)
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, login IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, eg do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Misuse and Infringements

eSafety Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported Coordinator. Additionally, all security breaches lost/stolen equipment or data must be reported to the senior leadership team.

Any eSafety incidents should be logged by the member of staff dealing with the issue. It can be accessed via the Greneway Dashboard (Google Sites). Any reported incidents are automatically forwarded to the ITC4learning Group who are available for advice if necessary. All incidents are reviewed at the termly meeting at which a Governor is present. (See Appendix 2 for more details)



Complaints
Complaints relating to eSafety should be made to the ITC 4 Learning Group or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed (see Appendix 2).

Inappropriate material
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ITC 4 Learning Group.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ITC 4 Learning Group, depending on the seriousness of the offence; investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct in line with the school behaviour policy and staff handbook.

Equal Opportunities

Pupils with additional needs
The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's' eSafety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies along with the associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through discussions with FoGS, presentations to the governors and involvement of the school council.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website / Twitter)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information evenings
    - Posters
    - Website - parent pages
    - Twitter postings

- Newsletter / School Blog - weekly eSafety ‘Top Tips’
- Surveys
- Provision of updated eSafety advice EG Digital Parenting Magazine
- Practical training session EG Parents drop-in session scheduled for Parent open afternoon.

Disposal of Redundant ICT Equipment Policy
All equipment to be disposed of goes to a recycler via County and we get a WEE certificate.

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making/ reviewing the eSafety policy through school council, staff meetings.

Acceptable Use Agreement: Staff, Governors and Visitors (Updated Sept 2015)

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ITC 4 Learning Group.

Ø I will only use the school's email / Internet / Intranet / Google Drive and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

Ø I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

Ø I will periodically change my password to ensure security and confidentiality.

Ø I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

Ø I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

Ø I will only use the approved, secure email system(s) for any school business.

Ø I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

Ø I will not install any hardware or software without permission of the Network Manager

Ø I will support the school approach to online safety and not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Ø I will not upload or add any images, video, sounds or text linked to or associated with the school or its community.

Ø Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

Ø I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

Ø I will respect copyright and intellectual property rights.

Ø I will ensure that my online activity, both in school and outside school, will not bring my professional reputation, or that of other, into disrepute.

Ø I will not use personal electronic devices (including smart watches) for personal use in public areas of the school between the hours of 8.30am and 3.30pm.

Ø I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. For example, I will preview recommended sites for use (RMTutor allows teaching staff to limit Internet sites used within a lesson).

Ø I will bring to the attention of the ITC 4 Learning Group any incidents related to eSafety and ensure that they are logged in the appropriate place.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature _____

Date _____

Full Name _____(printed)

Pupil Acceptable Use Agreement / E-Safety Rules (Updated July 2015)

- Ø I will only use ITC systems in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.

- Ø I will not download or install software on school technologies.

- Ø I will only log on to the school network/ Google with my own username and password.

- Ø I will follow the school's ITC security system and not reveal my passwords to anyone.

- Ø I will only use my school email address.

- Ø I will make sure that all ITC communications with pupils, teachers or others is responsible and sensible.

- Ø I will be responsible for my behaviour when using the Internet. This includes resources I access, the language I use and images I share.

- Ø I will support the school approach to online safety and not browse, upload or forward material that could be considered offensive or illegal.

- Ø If I accidentally come across any material that I am unhappy with or receive messages I do not like, I will report it immediately to my teacher.

- Ø I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.

- Ø Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher.

- Ø I will ensure that my online activity, both in school and outside school (including off site visits), will not cause my school, the staff, pupils or others distress or bring into disrepute.

- Ø I will respect the privacy and ownership of others' work on-line at all times.

- Ø I will not bring a Smartwatch to school as I am not permitted to wear one during the school day.

- Ø I will not attempt to bypass the Internet filtering system.

- Ø I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.

- Ø I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

User Signature

I agree to follow this code of conduct

Signature _____ Form _____

Date _____

Full Name _____(printed)

Year 6

Signature _____ Form _____

Date _____

Year 7

Signature _____ Form _____

Date _____

Year 8

Signature _____ Form _____

Date _____

Dear Parent/ Carer

ICT including the Internet, Google Sites/Drive, email, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT. At Greneway, we aim for all pupils to understand key eSafety issues and feel confident and able to make informed decisions about acceptable ICT use. These issues will be regularly highlighted within lessons and assemblies.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or ITC teacher.

Please return the bottom section of this form to school for filing.

Pupil and Parent/ carer signature

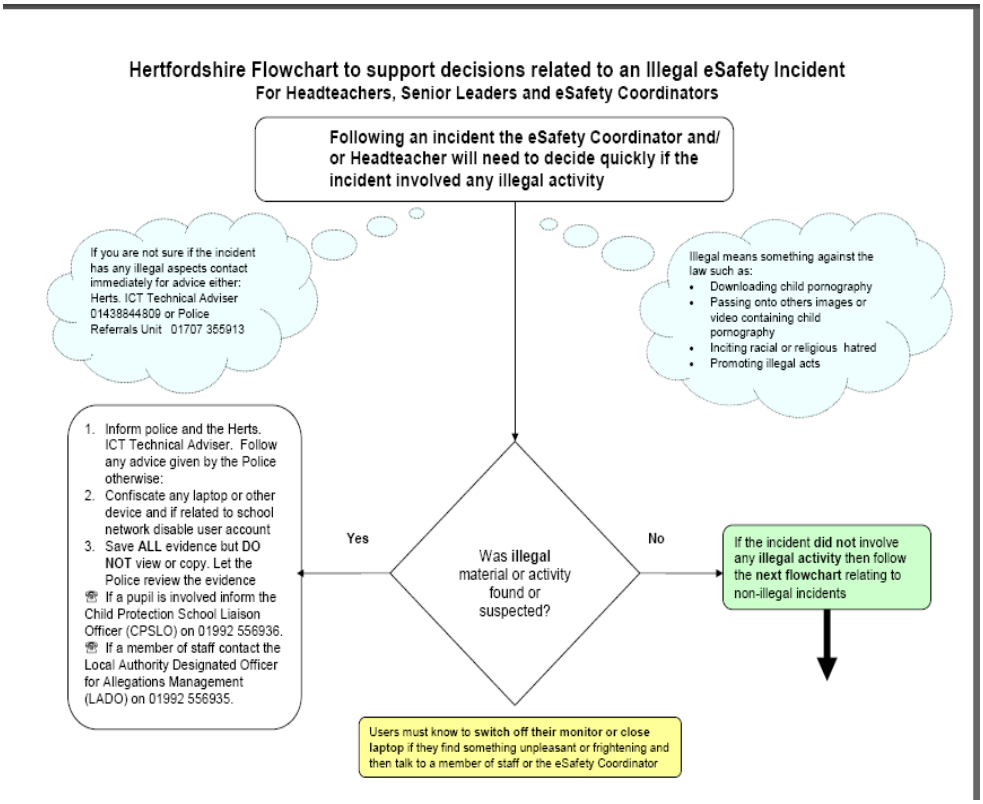
We have discussed this document and ……..(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at The Greneway School.

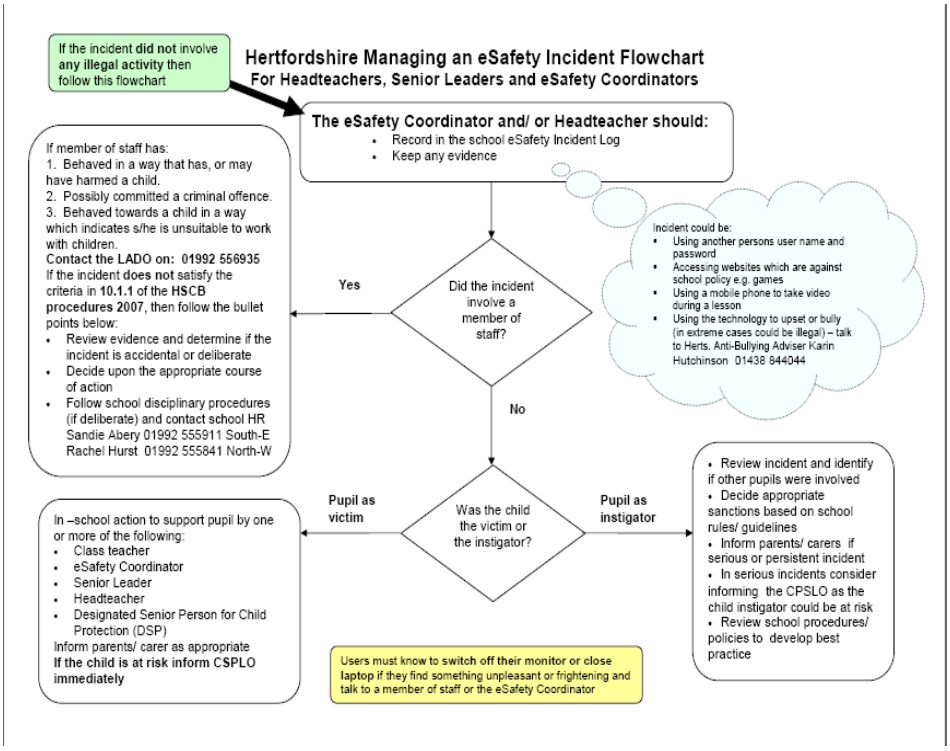
Parent/ Carer Signature …….

Pupil Signature…….

Form …… Date ……

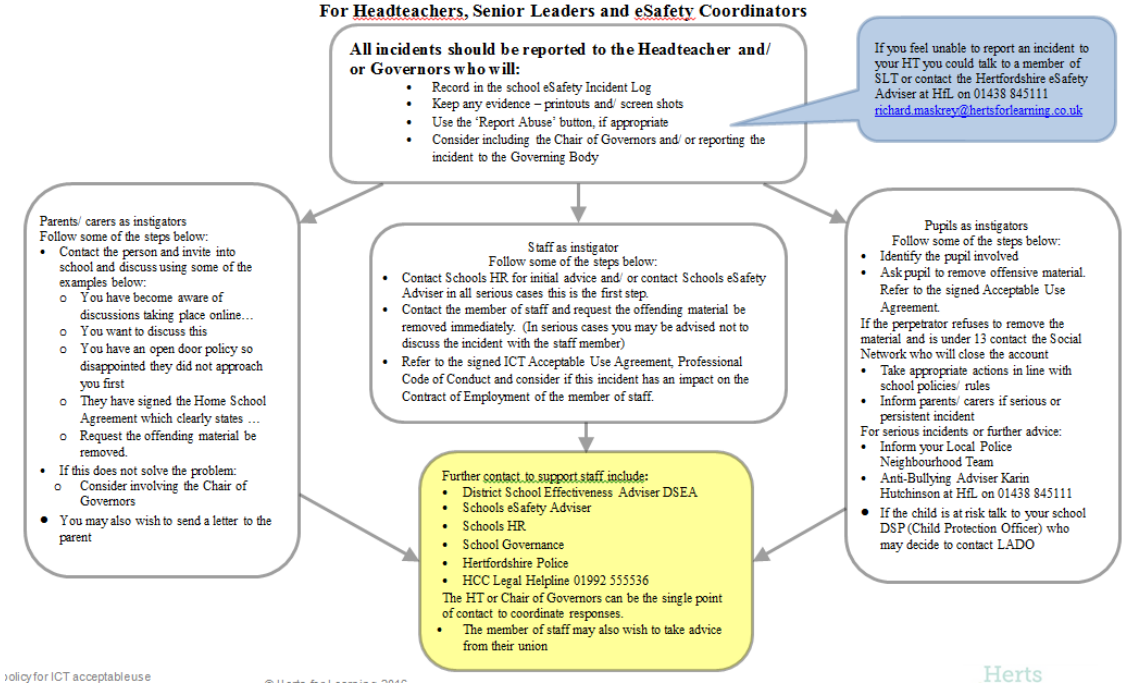
Appendix 2 – Flowcharts to support decisions relating to eSafety incidents





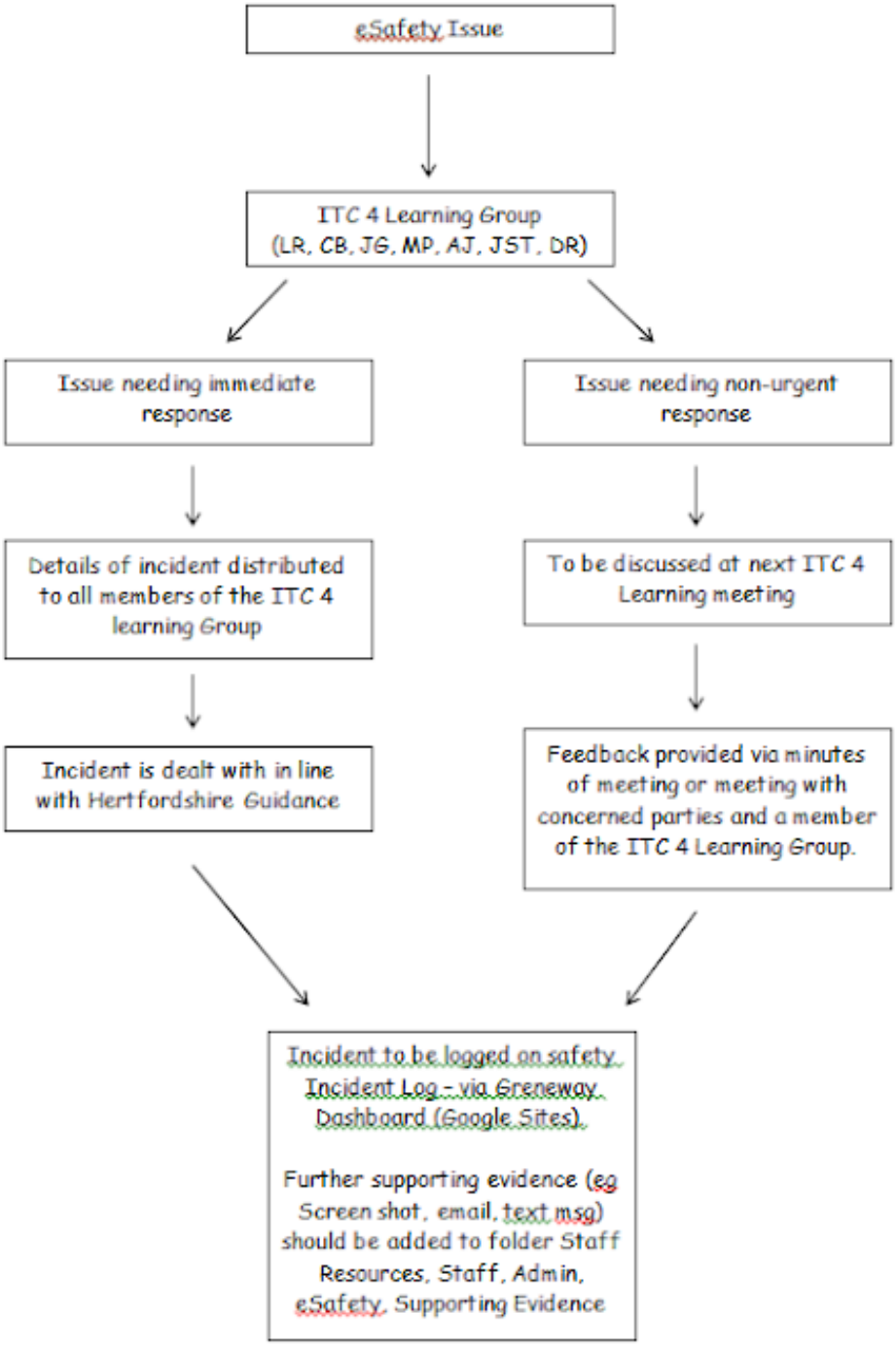
Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and eSafety Coordinators



olicy for ICT acceptable use

Herts


eSafety Issue
ITC 4 Learning Group
(LR, CB, JG, MP, AJ, JST, DR)
Issue needing immediate response
Issue needing non-urgent response
Details of incident distributed to all members of the ITC 4 learning Group
To be discussed at next ITC 4 Learning meeting
Incident is dealt with in line with Hertfordshire Guidance
Feedback provided via minutes of meeting or meeting with concerned parties and a member of the ITC 4 Learning Group.
Incident to be logged on safety Incident Log - via Greneway Dashboard (Google Sites).
Further supporting evidence (eg Screen shot, email, text msg) should be added to folder Staff Resources, Staff, Admin, eSafety, Supporting Evidence

Appendix 3
Greneway School E-Safety Overview

eSafety Curriculum 2017

Key Stage 2 Statutory Requirements:

- **Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.**
- **Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns and content and contact.**

Year 5

Key Objective:

- To promote safe use of the Internet
- To develop pupils as discerning users of the Internet

Coverage:

- Introduction to SMART using Sid's Online Safety Guide
- Design a poster to promote SMART
- Copyright Free Images
- Web Quests focusing on how results are selected and ranked - encouraging discerning use of sites/information.

PSHE Safety Day Activity:

- Kara, Winston and the Smart Crew

Year 6

Key Objective:

- To promote safe communication online
- To embed the use of advanced search in searching for copyright free images
- To promote critical thinking skills when searching on the Internet.

Coverage:

Use of Cyber café resources to explore

- Sending and receiving appropriate SMS text messages
- Sending and receiving appropriate e-mails
- Using social media appropriately [In conjunction with year 7 project]

Safe online searching - Critical Thinking Skills

PSHE Safety Day activity:

- How to search safely and with a critical eye.

Key Stage 3 Statutory Requirements:

- **Create, re-use, revise and re-purpose digital artefacts for a given audience, with attention to trustworthiness, design and usability.**
- **Understand a range of ways of using technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.**

Year 7

Key Objective:

- To promote awareness of safe use of social networking sites
- To revise safe use of the Internet
- To use advanced search to search and develop copyright free materials.
- To promote critical thinking skills through analysing the reliability of websites.

Coverage:

- Produce a Google Slide presentation for yr6 pupils on safe use of social networking sites.
- Produce a logo/corporate image' - making use of copyright free images
- Tree Octopus - looking at websites with a critical eye, assessing reliability.

PSHE Safety Day activity

- Produce an age appropriate guide to safe use of social networking sites

Year 8

Key Objective:

- To promote an understanding of data protection
- To promote an understanding of managing use of open, unfiltered Internet
- To promote an understanding of our 'Digital Footprint' and online presence
- To encourage pupils to be critical users of the Internet / online forums

Coverage:

- Linked webpage targeting advice about the use of unfiltered Internet.
- Data protection rights and laws / Copyright / Misuse of data (Accidental Outlaw)
- Review digital footprint and adjust Internet presence as appropriate.
- 'Fake News' Activity - Wales School Journey Week
- Critical Thinking activity linked to online communication.

PSHE Safety Day activity

Activities linked to a review of online friends, privacy settings and digital footprint.

Password Reminders for Staff

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you login. Do not include passwords in any automated logon procedures.
- Always change temporary passwords at first login.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you are aware of a breach of security with your password or account, inform the Network Manager (Nick, Martin or Darren) immediately.**
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.

Visit: https://howsecureismypassword.net/ to check the security of your password.

Greneway School eSafety Policy in Brief

- At Greneway School, we have an Acceptable Use Agreement which is reviewed at least annually, which all staff sign. Copies are kept on file. We use the LA model policy.
- Acceptable Use Agreements are signed by all staff/governors/pupils/visitors. We use an adapted version of the LA model agreements.
- Safe Handling of Data Guidance documents are available to all members of the school who have access to sensitive or personal data.

Personal or sensitive data must be encrypted if the material is to be romoved from the school.

- At Greneway, the network team can encrypt flash drives for this purpose HOWEVER, staff are encouraged not to take this data off site.
- At Greneway, we use the DfE S2S site to securely transfer CTF pupil files to other schools.
- At Greneway, we follow LA guidelines for the transfer of any other internal data transfer, using secure export to Local Authority Pupil Database.

Personal or sensitive material must be held in a lockable storage area or cabinet if in an unencrypted format (such as paper)

- At Greneway, we store such material in lockable storage cabinets in a lockable storage area.
- At Greneway, all servers are in lockable locations and managed by DBS-checked staff.
- At Greneway, we use follow LA back-up procedures and lock the tapes in a secure room. No back-up tapes leave the site on mobile devices.
- At Greneway, we use RM Support for disaster recovery on our admin server. (See N Rutter for further info re Disaster Recovery Plan)

Disposal: personal or sensitive material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At Greneway,we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- At Greneway, paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure.

- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access and Google access are moderated by N Rutter (Head of IT Support) and IT Support (DR, MP)

- Security policies are reviewed and staff updated at least annually and staff know to whom they should report any incidents where data protection may have been compromised. Staff have guidance documentation.