E-Safety and Online Policy

This policy should be read in conjunction with the following policies and guidance:

- *Safeguarding and Child Protection*
- *Data Protection*
- *Keeping Children Safe in Education 2023*
- *Guidance For Safer Working Practice For Those Working With Children and Young People in Education Settings 2022*

1. Introduction

1.1 .At Grangewood Independent, we understand the responsibility to educate our pupils on online safety issues (e-safety); 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.

1.2 Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

1.3 We understand that the breadth of issues classified within online safety is considerable and ever-evolving, but can be categorised into four areas of risk according to KCSIE 2023:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying), and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel any of our pupils, students or staff are at risk, it will be reported to the Anti-Phishing Working Group.

1.4 Internet, mobile and digital technologies in the 21st Century are essential resources 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.

1.5 Internet, mobile and digital technologies cover a wide range of resources including;

web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging, and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

1.6 Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, 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 technologies and that some have minimum age requirements (13 years in most cases).

1.7 The School holds personal data on learners, staff and others to help conduct day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

1.8 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.

1.9 Both this policy and the Acceptable Use Agreement (for all staff, Trustees and Governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, 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).

'Staff' applies to all Tutors, Teachers, Volunteers, Peripatetic staff, Trustees and Governors of the school.

2. Data Protection

Grangewood Independent holds a separate Data Protection Policy, including UK GDPR.

3. Filtering and Monitoring

3.1 Appropriate filtering and monitoring technology on school devices and school networks form part of our online safety.

Our school's filtering and monitoring technology is the responsibility of Mr. T. Roberts who is the school's Network Manager.

IT use is monitored using the following filtering and monitoring system: Sophos Firewall.

However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.

3.2 Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If staff are in any doubt as to whether the individual requesting such access is authorised to do so, their identification badge should be requested and contact Mr. Roberts to verify. Any ICT authorised staff member will be happy to comply with this request.

.3.3 ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

3.4 ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

3.5 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

3.6 Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

4. Breaches

4.1 A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware,

software or services from the offending individual (for pupils, please see Grangewood Behaviour Management Policy).

4.2 For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

4.3 Policy breaches may also lead to criminal or civil proceedings.

4.4 The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

4.5 The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

5. Incident Reporting

5.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or Business Manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher or Business Manager. The relevant responsible individuals in the school are as follows: **Mrs B. Roberts** (Headteacher), **Mr T. Roberts** (Business Manager).

5.2 Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

6. Computer Viruses

6.1 All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

6.2 Never interfere with any anti-virus software installed on school ICT equipment.

6.3 If a machine is not routinely connected to the school network, provision must be made for regular virus updates through the school IT team (Giotech).

6.4 If a virus is suspected on any school ICT equipment, the use of the equipment must be stopped and the ICT support provider contacted immediately (Giotech). Giotech will advise on what actions to take and be responsible for advising Mr. T. Roberts, who in turn will ensure the information is disseminated to others that need to know.

7. Data Security

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

7.1 Security of Confidential / Personal Data - Electronic and Paper

It is critical that the school considers the safety of confidential / personal data removed from a school site (electronic and paper).

- We will ensure that **ALL** staff are aware of how to handle sensitive or personal information.
- Storage devices such as USB sticks are best encrypted in their entirety.
- Staff laptops that hold personal data should have an encrypted 'container' created where all sensitive data should be stored.
- Backup media must always be kept secure.

7.2 Staff Guidance can be found in Grangewood Employees' Handbook.

7.3 Data Security in Schools - Dos and Don'ts.

- DO use privacy settings on social media sites to restrict access to your personal information.
- DO pay attention to phishing traps in email and watch for tell-tale signs of a scam.
- DO keep a clear desk, tidy confidential data away when not in use.
- DO consider whether it's necessary to use personal data to achieve your objective.
- DON'T open mail or attachments from an untrusted source.
- DON'T use data for any reason other than what it was originally collected for.
- DON'T leave data unattended.

8. Security

8.1 The school gives relevant staff access to its Management Information System (SIMs), with a unique username and password.

8.2 It is the responsibility of everyone to keep passwords secure.

8.3 Staff are aware of their responsibility when accessing school data.

8.4 Staff must read the relevant guidance documents and the Policy for ICT Acceptable Use.

8.5 Staff must read the relevant section on 'Safe Handling of Data', within the school's Employees' Handbook.

8.6 Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

8.7 Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

8.8 Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under control at all times.

8.9 It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed. This is particularly important when shared copiers (multi-function print, scan and copiers) are used.

9. Protective Marking of Official Information

9.1 Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

9.2 In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE**' or '**CONFIDENTIAL**'.

10. Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response.

10.1 The Senior Information Risk Officer (SIRO) and Information Asset Owner (IAO) at Grangewood is the Headteacher Beverley Roberts. This is a member of the senior leadership team who has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

10.2 The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

10.3 Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. The school's IAO should be able to identify across the school:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of.

10.4 As a result the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

10.5 However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The IAO in this school is Mrs. B. Roberts.

11. Disposal of Redundant ICT Equipment Policy

11.1 All redundant ICT equipment will be disposed of in a secure and safe manner. This should include the removal of the hard drive or sim card for the destruction of any personal data.

11.2 All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

11.3 Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
ico education-data

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

Data Protection Act – data protection guide
https://ico.org.uk/for-organisations/education/

11.4 The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will include:

Date item disposed of

Authorisation for disposal, including:
verification of software licensing
any personal data* likely to be held on the storage media?

How it was disposed of e.g. waste, gift, sale

Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

11.5 Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner Website
https://ico.org.uk/

Data Protection Act – data protection guide
https://ico.org.uk/for-organisations/education/

12. Online/Virtual Teaching

If the school needs to use online or virtual teaching the school will:

- ensure all relevant staff are briefed so they understand the policies and the standards of conduct expected of them.
- set clearly defined operating times for virtual learning.
- consider the impact that virtual teaching may have on children and their parents/ carers / siblings.

- determine whether there are alternatives to virtual teaching in 'real-time' - e.g., using audio only, pre-recorded lessons, existing online resources.
- ensure senior staff and DSL are able to drop-in to any virtual lesson at any time – the online version of entering a classroom; therefore the school will make these people aware of the virtual learning timetable and ensure they have the capacity to join a range of lessons.
- take into account any advice published by the local authority, or their online safety / monitoring software provider.

12.1 Whilst using online or virtual teaching staff should:
adhere to the school's policy on using online or virtual teaching as laid out here.

- be appropriately dressed.
- think about the background; photos, artwork, identifying features, mirrors - ideally the backing should be nondescript.
- ensure staff and pupils are in living / communal areas - no bedrooms.
- ensure all resources / videos are age appropriate.
- ensure that the Head Teacher is aware that the online lesson / meeting is taking place and for what purpose.
- avoid one-to-one situations - request that a parent is present in the room for the duration or ask a colleague or member of the SLT to join the session.
- only record lessons or online meetings with a pupil where this has been agreed with the Head Teacher or other senior staff, and the pupil and their parent / carer have given explicit written consent to do so.
- be able to justify images of pupils in their possession.

This means that adults should **not**:

- contact pupils outside the operating times defined by the Head Teacher.
- take or record images of pupils for their personal use.
- record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff).
- engage online while children are in a state of undress or semi-undress.

12.2 It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

12.3 Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage.

12.4 If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately.

12.5 Staff, parents and pupils should be aware of the standards of conduct required.

12.6 If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with the Head Teacher and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

13 Email

13.1 The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail 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 e-mail in relation to their age and how to behave responsibly online.

14. Managing E-Mail

14.1 The school endeavours to give all staff, Trustees and Governors their own e-mail account to use for all school business as a work-based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

14.2 Staff, Trustees and governors should use their school email for all professional communication.

14.3 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, e-mail histories can be traced. The school email account should be the account that is used for all school business.

14.4 As a general rule staff should not contact pupils, parents or conduct any school business using personal e-mail addresses.

14.5 All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

14.6 The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder.

14.7 Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher.

14.8 Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

14.9 E-mails created or received as part of the school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Therefore, e-mail accounts must be actively managed as follows:

- All e-mails of short-term value must be deleted.
- E-mails must be organised into folders and frequent housekeeping carried out on all folders and archives.

14.10 All pupils, from Reception to Year Six, have their own individual school issued Purple Mash logins which allow them to send and receive emails as part of the school's structured ICT/Computer Programme of Study. Pupils can also use a class/ group e-mail address under the supervision and direction of his/her class teacher.

14.11 All pupil e-mail users are expected to adhere to the generally 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 or upsetting e-mail.
- Staff must inform (the Head Teacher) if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing Programme of Study.
- In whatever way you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.
- The forwarding of chain emails is not permitted in school.

15. Sending E-Mails

15.1 If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section 17.

15.2 The school e-mail account should be used so that the originator of a message is clearly identified.

15.3 The number and relevance of e-mail recipients must be kept, particularly those being copied, to the minimum necessary and appropriate.

15.4 Attachments must not be sent forwarded unnecessarily. Whenever possible, the location path should be sent to the shared drive rather than sending attachments.

15.5 School e-mail is not to be used for personal advertising.

16. Receiving E-Mails

16.1 E-mails should be checked regularly.

16.2 An 'out-of-office' notification should be activated when away for extended periods.

16.3 Attachments from an untrusted source should never be opened; the School Business Manager should be contacted first.

16.4 E-mail systems should not be used to store attachments. Business related work should be detached and saved to the appropriate shared drive/folder.

16.5 The automatic forwarding and deletion of e-mails is not allowed.

17. E-Mailing Personal, Sensitive, Confidential or Classified Information

17.1 Where the conclusion is that e-mail must be used to transmit such data, express consent must be obtained from the Head Teacher to provide the information by e-mail. Caution should be exercised when sending the e-mail and these checks always followed before releasing the e-mail:

- Encrypt and password protect.
- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details have not been separately verified (usually by phone).
- Send the information as an encrypted document **attached** to an e-mail.
- Provide the encryption key or password by a **separate** contact with the recipient(s).
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt

18. Equal Opportunities: Pupils with Additional Needs

18.1 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 schools' e-Safety rules.

18.2 However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

18.3 Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

19. E-Safety Roles and Responsibilities

19.1 As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

19.2 The named e-Safety Safeguarding Officer in this school is **Beverley Roberts** who

has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

19.3 It is the role of the e-Safety Safeguarding Officer to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection), the UK Safer Internet Centre website and Childnet.

19.4 Senior Leadership and Governors are updated by the e-Safety Safeguarding Officer and all Governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

19.5 This policy, supported by the school's acceptable use agreements for staff, Governors Trustees, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, safeguarding, and health, safety and welfare, behaviour management (including the anti-bullying) policy and PSHE.

20. E-Safety in the Curriculum

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

20.2 The school has a framework for teaching internet skills in Computing/ICT and PSHE lessons.

20.3 The school provides opportunities within a range of curriculum areas to teach about Online Safety.

20.4 Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum

20.5 Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

20.6 Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.

20.5 Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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 Cybermentors, Childline or CEOP report abuse button.

20.6 Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the Computing/ICT curriculum (i.e computing scheme Purple Mash Y1/2 Unit 2.5, Y3/4 Unit 4.7, Y5/6 Unit 6.4, Y5/6 Unit 6.6).

21. E-Safety Skills Development for Staff

21.1 Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in the form of annual online awareness training provided through Educare and/or Smartlog, and as further required during regular safeguarding review in staff meetings (i.e. following updated risk assessment or changes to regulations/policies/guidance as they relate to e-safety).

21.2 Details of the ongoing staff training programme can be found on Educare/Smartlog admin dashboard, accessed by the Business Manager (Mr. T. Roberts).

21.3 New staff receive information on the school's acceptable use policy as part of their induction.

21.4 All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community *(report incident to* e-Safety Safeguarding Officer and log accordingly. *See Section 23.)*.

21.5 All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

22. Managing the School Online E-Safety Messages

22.1 We endeavour to embed Online e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

22.2 Online E-Safety posters will be prominently displayed in the ICT room.

22.3 The key online e-Safety advice will be promoted widely through school displays, newsletters, class activities and so on.

22.4 Awareness of the Safer Internet Day will be promoted every February.

23. Incident Reporting, E-Safety & Infringements

Incident Reporting

23.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or Safeguarding e-Safety Officer. Additionally, all security breaches, lost/stolen equipment or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

E-Safety Incident Log

23.2 Some incidents may need to be recorded if they relate to a bullying, extremism or racist incident (see the Safeguarding e-Safety Officer).

Misuse and Infringements

23.3 Complaints

Complaints and/ or issues relating to e-Safety should be made to the Safeguarding e-Safety Officer or Headteacher.

23.4 All incidents should be logged.

23.5 Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Safeguarding e-Safety Officer.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an 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.
- Users are made aware of sanctions relating to the misuse or misconduct through the Employees Handbook and Induction process.

24. Internet Access

24.1 The internet is an open worldwide communication medium, available to everyone, 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.

25. Managing the Internet

25.1 The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

25.2 Staff will preview any recommended sites, online services, software and apps before use.

25.3 Searching for images through open search engines is discouraged when working with pupils (have prepared resources in a folder or document ahead of lessons and activities).

25.4 If Internet research is set for homework, specific sites should 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.

25.5 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

25.6 All users must observe copyright of materials from electronic resources.

26. Internet Use

26.1 Personal, sensitive, confidential, or classified information must not be posted or such information disseminated in any way that may compromise the intended restricted audience.

26.2 Names of colleagues, pupils, others, or any other confidential information acquired through working at the school must not be revealed on any social networking site or other online application.

26.3 On-line gambling or gaming is not allowed.

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

27. E-Safety and the Prevent Duty

27.1 Grangewood takes seriously its responsibility to ensure that children are safe from terrorist and extremist material when accessing the internet in school and therefore has suitable filtering in place.

27.2 As with other online risks of harm, every teacher is made aware of the risks posed by the online activity of extremist and terrorist groups. General advice and resources on internet safety are available on the UK Safer Internet Centre website.

28. Infrastructure

28.1 This school is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

28.2 Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

28.3 The school does not allow pupils access to internet logs.

28.4 The school uses management control tools for controlling and monitoring class and ICT suite computers.

28.5 If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Safeguarding e-safety Officer or teacher as appropriate.

28.6 It is the responsibility of the school, by delegation to the network manager (Giotech), to ensure that anti-virus protection is installed and kept up to date on all school machines.

28.7 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 neither the school's responsibility nor the IT support team's to install or maintain virus protection on personal systems. If pupils wish to submit electronic work it must be emailed to the class teacher's class email.

28.8 Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Head Teacher.

28.9 If there are any issues related to viruses or anti-virus software, the Business Manager should be informed immediately through the school office.

29. Managing Other Online Technologies

29.1 Online technologies (including social networking sites and generative AI tools, 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.

29.2 All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

29.3 Pupils are taught 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.

29.4 Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

29.5 Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

29.6 Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

29.7 Our pupils are asked to report any incidents of Cyberbullying to the school.

29.8 Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platforms or other systems approved by the Head Teacher.

29.9 Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

30. Parental Involvement

30.1 We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. Class teachers consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to the school.
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
  - ✓School website information
  - ✓Newsletter items
  - ✓Posters

31. Passwords and Password Security

31.1 Passwords

- Personal passwords must always be used by staff members.
- Personal passwords must be entered each time staff logon. Passwords must not be included in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Passwords must be changed whenever there is any indication of possible system or password compromise.
- Passwords or encryption keys must not be recorded on paper or in an unprotected file.
- Personal passwords should only be disclosed to authorised ICT support staff when necessary, and never to anyone else. All personal passwords that have been disclosed must be changed once the requirement is finished.
- Staff should never tell a child or colleague their password.
- Mr T. Roberts must be informed immediately if there is a breach of security with password or account information.
- Passwords should contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 5 school days.

31.2 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 private and not to share with others. Staff and pupils are regularly reminded of the need for password security.

31.3 All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.

31.4 Class teachers are provided with an individual network, email, learning platform and Management Information System log-in username.

31.5 Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers, or others.

31.6 Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

31.7 Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).

31.8 In our school, all ICT password protocols and procedures are the responsibility of Mr. T. Roberts and all staff and pupils are expected to comply with the policies at all times.

32. Zombie Accounts

'Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access.

33. Personal or Sensitive Information

33.1 Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from a personal PC or removable media equipment is kept secure, and any portable media is

removed from computers when not attended.

- Ensure 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 that is disclosed or shared 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 that is copied, scanned or printed. This is particularly important when shared copiers (multi-function print, 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 the Head Teacher.
- Personal, sensitive, confidential, or classified information, or disseminate such information must not be posted on the internet, or such information disseminated in any way that may compromise its intended restricted audience.
- Screen displays must be kept out of direct view of any third parties when 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 labelling.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Hard copies of data must be securely stored and disposed of after use in accordance with the document labelling.

34. 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

34.1 For guidance on how to encrypt files see the school SIRO.

35. Remote Access

- You are responsible for all activity via your remote access facility

- 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, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g., 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
- Always protect school information and data, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

36. Safe Use of Images

36.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. 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 (also see Grangewood Media, Photography and Filming Policy).

- 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 pupils, staff and others without advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

36.2 Consent of Adults who work at the School

- Permission to use images of all staff who work at the school is sought on induction.

36.3 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
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e., exhibition promoting the school
- general media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

36.4 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, e.g., divorce of parents, custody issues, etc.

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

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

36.7 Only the Business Manager, Headteacher or School Secretary has authority to upload to the internet.

37. Storage of Images

- Images/ films of children are stored on the school's network and school production DVDs.
- 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 or other online school resource.
- The School Secretary and Business Manager have the responsibility of deleting the images when they are no longer required.

38. Webcams and CCTV

- The school uses CCTV for security and safety. The only person with

access to this is the School Business Manager. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance

https://ico.org.uk/media/about-the-ico/consultations/2044/draft-cctv-cop.pdf

- We do not use publicly accessible webcams in school.
- Webcams will not be used for broadcast on the internet without prior parental consent.
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices (Grangewood Media, Photography and Filming Policy, Grangewood Safeguarding Policy).
- 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).

39. 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 (or by a parent/carer, if pupil involved in remote learning arranged by the school) 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 to endpoints beyond the 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 (previously CRB) 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.

40 School ICT Equipment including Portable & Mobile ICT Equipment and Removable Media

40.1 School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or another portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all school ICT equipment to the school. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the Headteacher or Business Manager
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

40.2 Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or 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, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by Giotech, fully licensed and only carried out by Giotech
- In areas where there are likely to be members of the general public, portable 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

40.3 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. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. 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.

40.4 Personal Mobile Devices (including Phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device
- Pupils are only allowed to bring personal mobile devices/phones to school after written permission has been obtained from parents/ carers and agreement sought from the Headteacher. At all times the device must be switched onto silent and handed into the School Office as soon as the pupil is onsite.
- 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
- Never use a hand-held mobile phone whilst driving a vehicle

40.5 School Provided Mobile Devices (including Phones)

- The school does not provide any mobile devices

40.6 Telephone Services

- You may make or receive personal telephone calls provided:
  1. They are infrequent, kept as brief as possible and do not cause annoyance to others
  2. They are not for profit or to premium rate services
  3. They conform to this and other relevant school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available through the school office and by each school telephone handset. If you do not have a copy, please ask Mr. Roberts.

40.7 Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to section 33.

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

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely.

41. Social Media

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

- Our school uses Twitter to communicate with parents and carers. **Terry Roberts** is responsible for the oversight of all postings on this technology and monitors responses from others
- Staff should not access their personal social media accounts using school equipment during school hours
- Pupils are not permitted to access their social media accounts whilst at school
- Staff, Trustees/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, Trustees/Governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, Governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

42. Servers

Grangewood Independent School abides by the following criteria:

- Server is kept in a locked and secure environment
- Access rights are limited
- Server is password protected
- Server has security software installed appropriate to the machine's specification
- Data is backed up regularly
- Back up media is stored off-site and securely monitored by school's IT support (Giotech).

43. Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended.

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

43.1 It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

44. Writing and Reviewing this Policy

44.1 Staff Involvement in Policy Creation

Staff and Governors have been involved in reviewing the Policy for ICT, E-Safety and Acceptable Use, through staff meetings and governor policy review.

44.2 Review Procedure

- There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them.
- There will be on-going opportunities for staff to discuss with the IAO any issue of data security that concerns them.
- This policy will be reviewed every two years and consideration will be 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.
- This policy has been read, amended and approved by the staff, headteacher and Governors.

Signed:

Member of Governing Body:  Date: SEPT 2023

Chair of Governors: JONES AGYEMAN Date: **Sept 2023**

Next Review Date: Sept 2024

Grangewood Independent School

Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own, or others, details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will respect the privacy and ownership of others' work on-line at all times
- I will not sign up to online services until I am old enough

Grangewood Independent School

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's Class Teacher or the Headteacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂----------

Parent/ carer signature

We have discussed this document with ..... (Child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at Grangewood Independent School.

Parent/ Carer Signature .....

Class ..... Date .....

Reviewed: **Sept 2023**, Oct 2022, Sept 2021, Jun 2020, Apr 2019, Sept 2018, Nov 2017, Mar 2017, Jul 2015

Grangewood Independent School

Parent/Carer
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all parents/carers are aware of their parental responsibilities regarding using any form of ICT in relation to the school. All parents are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with your child's Class Teacher, or the Headteacher.

- I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.
- I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.
- I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).
- I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.

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

Signature ..... Date .....

Full Name ..... (Printed)

Child's Name .....

Relationship to child .....

Signature ..... Date .....

Full Name ..... (Printed)

Child's Name .....

Relationship to child .....

Grangewood Independent School

Staff, Governor, and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, 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 Mr Roberts (School Business Manager).

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement:

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

For my professional and personal safety:

- I will follow requirements for data protection as outlined in the Online Safety and Data Protection Policy.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will follow requirements for data protection as outlined in the Online Safety and Data Protection Policy.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 6pm, except in the staff room or school office.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will not use personal email addresses on the school ICT systems unless expressly given permission by the Headteacher.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

User Signature

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines, and agree to the above Acceptable Use Agreement / E-Safety Rules.

I agree to follow this code of conduct.

Signature ..... Date .....

Full Name ..... (Printed)

Job title .....

HELP AND SUPPORT

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on e-Safety:
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/

Test your online safety skills http://www.getsafeonline.org

Information Commissioner's Office – www.ico.org.uk

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015 – this is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision –
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

For additional help, email school.ictsupport@education.gsi.gov.uk

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic

transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services