Rowan Preparatory School
Technology Policy

Prepared by	Vicky Langham Ian Jackson	Business Manager IT & Facilities Manager
Owned by	Sarah Raja	Headmistress
Applies to	Staff ¨	Students ¨
	Parents ¨	Governors ¨
Reviewed:	October 2024	
Next Review:	October 2025	

Table of Contents

Introduction

In today’s society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

This Technology Policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and all computer and tablet technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the ‘duty of care’, which applies to everyone working with children.

There are a number of themes that run through all the policy areas addressed in this document. Firstly there is the need to balance control against developing responsibility. Schools within United Learning must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions about how to use technology as well as to feel able to report any concerns.

Secondly there is a need to find a balance between a set of highly secure technology systems and usability. School leadership teams must be clear about how much freedom users should have and the risks these entail. Finally there is the need to chart a sensible course to solve problems of misuse of technology; technical solutions can be used, for example to prevent student access of gaming sites during lessons but at heart these may be behaviour or cultural concerns that fundamentally should be tackled as such.

Breaches of the technology policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the consequences that inappropriate use of technology can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The Technology Policy is essential in setting out how your school plans to develop and establish a safe approach to the use of Technology, to identify core principles which all members of the school community need to be aware of and understand, and to enable the school to develop an effective and safe online community.

Scope of the Technology Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school Computing systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such an extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. Sanctions employed align with the school's wider behaviour and bullying policies.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school with regards to the use of technology:

Governors:

Governors are responsible for ensuring that a school complies with its legal obligations. Governors are responsible for the approval of the Technology Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-safety Governor who liaises closely with the designated Child Protection Governor. The role of the E-Safety *Governor* will include:

- regular meetings with the Head of Innovation and Technology
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Governors meetings

Headmistress and Senior Leaders:

- The Headmistress has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Head of Innovation and Technology .
- The Headmistress and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *United Learning HR* disciplinary procedures).
- The Headmistress is responsible for ensuring that the Head of Innovation and Technology and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headmistress will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the Head of Innovation and Technology.

Head of Innovation and Technology : Alex Wright

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school technology policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with United Learning / relevant bodies
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governor's meetings to provide updates
- reports regularly to Senior Leadership Team

IT & Facilities Manager: Ian Jackson

The IT & Facilities Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and complies with Guidance from United Learning technology department.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headmistress and Head of Innovation and Technology for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of the safe use of technology and e-safety matters and of the current school technology policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headmistress and Head of Innovation and Technology for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities

- pupils understand and follow the technology and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the technology policy including the impact of initiatives. The group will be responsible for regular reporting to the Governing Body.

Members of the E-safety Group will assist the Head of Innovation and Technology with:

- the production / review / monitoring of the school technology policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision

Membership of this groups is: Headmistress, IT & Facilities Manager, Head of Innovation and Technology, DSL (Designated Safeguarding Lead)

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Technology Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the school

Breaches of the Policy

By Students

Any breach of this policy may lead to disciplinary action being taken against the pupil/s involved in line with the school's Disciplinary Policy.

By Staff

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with United Learning's Disciplinary Policy. A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or United Learning or any illegal acts or acts that render the school or United Learning liable to third parties will result in disciplinary action appropriate to the severity of the breach.

By Contracted Providers of Services

Contracted providers of services to the school/ United Learning must inform the schools/ United Learning immediately of any breaches of this policy by their staff so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school/ United Learning. Any action against breaches should be according to contractors' internal disciplinary procedures

E-Safety Policy

Introduction

The e-safety policy is a key element of the Technology Policy as it is about the safe and responsible and ethical use of online technologies. It covers accessing online resources through computers, tablets, smart phones and any other internet enabled device safely and effectively. In conjunction with the Social Media policy, it includes new social media tools and other emerging trends. It should cover a range of issues and not condemn the use of tools but rather address how to use them safely. This should include how to comment appropriately in many different forums, including social media and not being just a bystander. An essential part of this is how to report concerns, online and offline.

The policy will outline who will deliver the training, in which subject area and to which parts of the school community. It also references how the effectiveness of the processes is monitored

Key Personnel

The E -safety Policy is reviewed annually by the Headmistress and Head of Innovation and Technology with the Designated E safety Governor.

The Head of Innovation and Technology will arrange appropriate training for staff, pupils and parents/ carers.

Areas of risk

Child Protection	Children are exploited by sex offenders Children upload inappropriate content online Children publish personal information which identifies them either overtly or covertly (location metadata in images or messages) Staff do not understand the technology and under (or over) estimate the risk
Staff Protection	Staff post comments or images which compromise their professional integrity Staff lack of understanding of new online tools puts them at risk.
ISI Inspection	Lack of understanding of the e-safety policy by staff, students or governors can prevent a school from achieving an excellent or outstanding inspection judgement.

Scope

This e-safety policy should be read in conjunction with other policies with the over-arching Technologies Policy but with particular reference to the Mobile Devices Policy, Social Media Policy and Internet Filtering Policy

Policy Statements

Communicating with children electronically

Email is the only approved methods of electronic communication between staff and students.

Education – pupils

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages accross the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT & Facilities Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers   (see appendix for further links / resources)
- Distributing the Vodaphone Digital Parenting Magazine termly

Education – The Wider Community

The school may provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Inviting other organisations to join staff training sessions
- E-Safety messages targeted towards grandparents and other relatives as well as parents.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Head of Innovation and Technology will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Head of Innovation and Technology will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at external training courses
- Participation in school training / information sessions for staff or parents

E-safety Information

Internal resources

Pupils & staff are provided with e-safety information through briefings form the Head of Innovation and Technology and resources made available for use on the Computing curriculum area. There are a variety of e-safety links within the Computing lesson folders.

Key Stage 2 pupils can access E safety booklets, which are used in PSHE and Computing lessons, on the Pupil Resources area. Pupils also have a copy of the booklet in the PSHE books and their Computing folder.

Key Stage 1 and EYFS pupils resources, including those for E safety, are accessed by teaching staff and work is kept in the yellow Computing folder for each class.

Staff and Parents can locate e-safety information via the school Parent Portal and public website.

Public website: http://www.rowanprepschool.co.uk/About-us/E-safety

- **External resources**

  The E safety pages maintained on our public website and the Parent Portal contains external sources of reliable information on the safe use of the internet and links to parental information sites including the following:-

  CEOP and the Parent Zone
  Childnet International
  UK Safer Internet centre

Reporting Procedures

- **Internal reporting**

Pupils are briefed to report any issues or concerns to their class teacher or to Miss Roberts Holmes, Head of Innovation and Technology. Concerns raised will be shared with staff through the normal school channels for this as set out in our Safeguarding policy. Investigations where appropriate will be facilitated by the IT & Facilities Manager.
Staff report any concerns relating to E-safety to either the Head of Innovation and Technology or directly to a member of SLT. Annual staff training on Safeguarding Children includes E-safety.

Logs are maintained of concerns raised as part of Rowan's safeguarding children / child protection procedures.

- **Monitoring Reports**
  Logs of child protection issues raised and actions taken are regularly reviewed by the Headmistress and shared with the LGB, any issues relating to technology / e-safety can be identified.

  External Reporting
  The "Report Abuse" link to the CEOP reporting mechanism is included on the Rowan website. Staff are also aware of other useful links for reporting, Childline (http://www.childline.org.uk), the Online Professional Helpline (http://www.saferinternet.org.uk/about/helpline).

Monitoring Success

The success of the E safety policy is regularly monitored through review with pupils of their understanding. This includes the use of formal questionnaires towards the end of the summer term reflecting the 6 part e-safety course that girls form Nursery to year 6 undertake throughout the year.

In addition parental feedback is gathered as part of the regular parent forums and surveys.

Mobile Device Policy

Introduction

The majority of staff, for security and practical reasons, carry a mobile phone, and for these reasons their use is allowed in school. However, as we are a working community, we need to have regulations governing the use of Wi-Fi and 3G/4G enabled devices so that incoming communications do not interrupt lessons and so that students do not use them unnecessarily and disrupt the effective operation of the school.

This Policy applies to 'standard' mobile phones as well as smart phones such as iPhones, Blackberries, Android and Windows phones, and other 3G/4G and WiFi enabled devices such as iPads, iPods, tablets and laptops. Use of mobile devices by members of staff and students is regulated, in accordance with Group policy and recognised professional standards of acceptable practice.

This policy should be read as part of the school's Technologies Policy in conjunction with the school's Acceptable Usage policy for Technologies. Guidelines for staff and pupils relating to mobile devices are published and reviewed annually.

The school accepts that staff are permitted to bring such devices to school but their use is restricted as detailed in this policy. Pupils however are not permitted to have such devises in school, if they do need to bring them. E.g. for safety when travelling to and from school they must be left in the school office for the duration of the school day.

This policy applies to all members of the school community, including those in our EYFS setting.

This policy is reviewed annually by the school senior leadership team, who will report to the Local Governing Body on its implementation on a regular basis.

The school is committed to ensuring that the implementation In accordance with the school's Provision of Information Policy, the policy should be made available on the school's website and in hard copy from Reception. It should be read in conjunction with:

- Behaviour and Discipline Policy
- Care and Consideration: Anti-Bullying Policy
- Exclusion, Expulsion, Removal and Review Policy

The school is committed to ensuring that the implementation of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the school's own Equal Opportunities Policy.

Key Personnel

This policy will be reviewed annually by the Headmistress.

The IT & Facilities Manager will provide technical expertise on mobile digital devices, their use and risks.

Area of Risk

Child Protection:	Pictures of children on the at risk register become associated with the school through linked social media platforms
Bullying:	Use of mobile technology can make bullying more pervasive and difficult to monitor
Staff Protection	Content recorded in lessons, whether overtly or covertly, on mobile devices may cause distress to staff, especially when uploaded to social platforms.

Procedures

A common sense approach should be followed regarding the use of 3G and Wi-Fi enabled mobile devices. Teachers should always have the ability to override rules against mobile device use, where common sense prevails, although the following guidelines should be used:

Times and locations where mobile devices may be permitted

- Under direction from a member of staff, students may use either school owned cameras or IPADs to make an appropriate record of their work.
- No content recorded on a personal device should be uploaded to a social media, video sharing (such as YouTube) or photograph sharing site (such as Flickr), without the permission of those being filmed, including members of staff. Doing so could result in disciplinary action.

Times and locations where mobile device use is not permitted

- Mobile devices should be switched off or muted and in airline mode during lessons
- Parental agreement must be obtained for the school using its own devices to film students on occasion for internal use.

Sanctions for Misuse of Mobile Devices

The school will apply appropriate sanctions to any student or member of staff who uses their mobile phone, or other device, for bullying, intimidation, or for keeping, or disseminating inappropriate text or images.

Security of Mobile Phones and other electronic devices

Students and staff are advised to have their phones/iPods/iPads security marked

The school does not accept responsibility for personal mobile phones or other electronic communication devices or entertainment systems. Staff should be informed that mobile phones and other such devices are not covered by the organisation’s insurance policy. Staff should be advised to keep valuables with them or in the staffroom, though their security there cannot be guaranteed.

Cyber Bullying

Instances of cyber bullying will be punishable in accordance with the school’s Anti-Bullying Policy and may even result in exclusion or expulsion (or in disciplinary action, in the case of staff – refer to staff bullying and harassment policy).

Dealing with Inappropriate Content on Mobile Devices

If a teacher suspects or is informed that a student has inappropriate content on their mobile device then the teacher will confiscate the device. The Deputy Head will investigate the matter and report to the Headmistress. During their investigations, if the student is formally interviewed, this will be with another member of staff present. A member of staff may investigate content on the mobile device in line with the school’s search policy. The student’s parents may also be invited to attend the interview. In line with the school’s policy on Exclusion, Expulsion, Removal and Review, the student may also be suspended whilst the allegation is being investigated.

Any instances of inappropriate images of children or young people on staff mobile devices must be reported immediately to the Headmistress or in her absence one of the Designated Safeguarding Leads.

Use of mobile devices: guidelines for staff use (photographs and videos)

Staff working in the EYFS setting are specifically prohibited by EYFS regulations from using their personal devices (cameras, mobile phones, IPADS) to take photographs or videos of children in the EYFS setting for any reason. Only school devices may be used. Rowan has decided to extend this to be policy throughout the school.

Staff must under no circumstances ever use any photographs of students for anything other than strictly professional purposes. They must never upload photographs or videos of any students onto the internet or social media site. The only exception is for the marketing department to use photographs of students, where parents have given consent, on the school's own website or other school managed social media platforms.

After taking photographs of students on mobile devices, staff should not store these for any longer than necessary, and once copied onto the school network should be deleted from the mobile devices.

Before printing any photographs of students in any external publication (e.g. local or national newspapers), parents must give permission for the student's photograph and/or name to be used.

Electronic Devices Policy - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil/ student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headmistress (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that the Headmistress should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

Responsibilities

The Headmistress is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headmistress will need to authorise those staff who are allowed to carry out searches.

This policy will be reviewed by the E safety group

The Headmistress has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's e-safety policy

Members of staff authorised by the Headmistress to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy relating to Search and Deletion:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

If pupils / students breach these roles:

The sanctions for breaking these rules can be found in the Behaviour Policy

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Searching with consent - Authorised staff may search with the pupil's consent for any item.

Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or

whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices

Audit / Monitoring / Reporting / Review

The Headmistress will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed with the E-Safety Governor at regular intervals.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance

Social Media Policy

INTRODUCTION

The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that United Learning staff and contractors are expected to follow when using social media.

It is crucial that students, parents and the public at large have confidence in schools' decisions and services. The principles set out in this policy statement are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school and United Learning are safeguarded.

This policy statement also aims to help staff use social media with minimal professional risk. Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Key Personnel

The Headmistress will be responsible for reviewing and authorising the policy.

Technical expertise on social media, its use and risks, will be provided from United Learning technology team via the Technology Business Partner.

Scope

This policy covers personal use of social media as well as the use of social media for official United Learning/ school purposes, including sites hosted and maintained on behalf of the either.

This policy applies to personal web presences such as social networking sites (for example *Facebook*) blogs and microblogs (such as *Twitter)*, chatrooms, forums, podcasts, open access online encyclopaedias (such as *Wikipedia*), social bookmarking sites (such as *del.icio.us*) and content sharing sites (such as *flickr* and *YouTube*). The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal Framework

United Learning is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of United Learning are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

Staff should also be aware of the guidance and sanctions contained within the United Learning Disciplinary Policy

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998 (see Data Protection Policy) and General Data Protection Regulations (2018).
- Information divulged in the expectation of confidentiality
- School or United Learning business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

Schools and United Learning could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the schools and United Learning liable to the injured party.

Professional Use of Social Media

The school maintains a presence on various social media sites as they provide very effective additional channels of communication with parents/ carers, students and the wider community.

This is not without risk, however and staff members should be aware that;

- services such as X, Instragram are in the public domain and are regularly used by journalists, students, parents and employers
- submissions can take on a life of their own once sent by users, who should not rely on being able to delete them
- Schools and United Learning may re-tweet the submissions of staff members to their wider following
- Students or parents may retweet comments and pictures which directly relate to them, their family or their friends.
- The ability to post anonymous comments to social media platforms, such as Twitter, may result in offensive or upsetting comments being directed at schools or staff.

Policy statements

Staff members must not upload video content to hosting services (such as YouTube) without sign off from the / Head teacher. This is for reasons of safeguarding and for maintaining the reputation of the school and United Learning. Likewise, staff members must not make use of any social media service with students apart from the school's Learning Platform or the United Hub, unless a pedagogical business case and associated risk assessment is agreed.

Staff members should maintain a professional persona through any use of social media for work purposes. User names should be formal (e.g. @MrSmith_SchoolName) or anonymised (e.g. @PE_SchoolName). The latter option also distances the user from their real-life identify and makes online bullying less likely.

All professional submissions to social media sites must show the school and/or United Learning in a positive light and should be written without ambiguity or any rhetorical device (such as sarcasm) which might be misinterpreted. It is surprisingly easy for even the gentlest of humour to be read differently than intended when parsed through abbreviated media such as Twitter.

Staff members must not enter into dialogue using social media such as Twitter, which schools and United Learning are using purely as a one-way channel for distributing news. Any attempt by other users to interact with staff members via such services should be reported to the Headmistress for advice and resolution. The simplest option is usually to take such issues offline. Even the simple act of responding to a pupil's tweeted question confirms that pupil attends the school, links to their wider digital identity and photographs of them and does so in a purposefully public forum.

Staff members should exercise professional judgement when using social media. If new to social media it is good practice to ask a senior colleague's opinion before posting an update to a social media service. If in doubt over the appropriateness of a submission, the best option is not to make it. Appropriate disciplinary action will be taken should a member of staff make a submission which brings the school or United Learning into disrepute.

Any images submitted to a social media site should be chosen carefully and should show the school positively.

Images of students must only be uploaded with exceptional caution; no individual or close up images should be used where the student could be identified. Likewise, no image which might reasonably be judged to cause embarrassment to the student should be published. 'Over the shoulder' images (where individuals are not recognisable) or group shots of 3 or more students are safest. Staff should seek advice from a senior colleague before publishing images of students wearing PE kit

Images of individual staff should only be uploaded with their consent and no image which might reasonably be judged to cause embarrassment to the member of staff should be published.

Individual students should not be identifiable through submissions to social media sites, for safeguarding reasons. For example, "Excellent piece of work created by Isobel in Y4" is acceptable, whereas including Isobel's surname is not. Any submission that includes an image of a student must not make reference to the student's first, sur- or full name under any circumstances.

Strong password security must be maintained and regularly changed for any social media account, to prevent it from being hi-jacked and misused. Passwords should never be written down. A combination of upper and lower case characters should be combined with numerals. The potential for hi-jacked accounts to bring schools and United Learning into disrepute is significant and responsibility for account security lies with the staff member who controls it. Staff should be cognisant that such accounts are likely to be targeted by pupils for precisely this purpose.

Devices used to post content to social media platforms should be password protected to prevent third parties from posting on your behalf
Fraping (or Facebook raping) is where a third party changes the a person's status or post inappropriate content to a social media platform with their consent or knowledge. The consequences can be long term and damaging.

Personal Use of Social Media

It is reasonable for members of staff to maintain personal web presences in their lives beyond their school life. Indeed, in 2012 over 53% of the UK population had a Facebook account.

School staff, however, occupy an almost unique professional position due to their work with children and the moral credibility they must maintain. There have been several recent cases where school staff have suffered serious professional consequences as a result of poor judgement in the use of social media.

It is worth considering that information (text, images, video) held in web presences;

- is never completely private and can very easily enter the public domain
- can be misinterpreted by audiences it was not originally intended for
- may persist beyond your wishes
- might be copied and used by third parties without your consent

It is therefore vital that use of social media in staff's lives beyond the school be totally separated from their professional identity. However, staff should be aware that even if this separation is strictly adhered to, it remains relatively easy for people (students, journalists, future employers etc.) to connect staff in schools with 'private' social media presences.

Policy statements

- Staff members are advised to exercise caution in identifying themselves as employees of the school or United Learning in their personal web presences. They must not purport to represent the views of either organisation on personal social media.
- Staff members are advised not to have contact through any personal social medium with any student or member of a students' family, unless the students are family members.
- Staff members should not put themselves in a position where extreme political, religious or philosophical views expressed via social media conflict with those of a public institution such as a school.
- Staff members should not use social media to document or distribute evidence of activities in their private lives that may bring the school or United Learning into disrepute.
- Staff members must decline 'friend requests' from pupils they receive to their personal social media accounts.
- On leaving the school's/ United Learning's service, staff members must not initiate contact with former pupils by means of personal social media sites whilst that pupil is under the age of 18.
- Staff members must not initiate contact with former pupils by means of personal social media sites whilst that pupil is under the age of 18 or in full time secondary or 16 to 19 education.
- Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties must not be discussed on their personal web presence.
- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity from work.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites.
- Staff members must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or the school/ United Learning.

Social Networking Standards

Below sets out the standards expected of all United Learning employees when using social networking sites:

DO

- **Act responsibly at all times**. Even if you do not identify your profession or place of work, please be aware that your conduct online could jeopardise any professional registration and/or your employment.
- **Protect your own privacy**. Think through what kinds of information you want to share online and with whom you want to share this information. Adjust your privacy settings accordingly. Remember that the more personal information you share online, the more likely it is that something could have a negative impact on your employment. Think about managing your online friends by restricting what kind of information you give them access to.
- **Remember everything is public**. Even with the highest level of privacy settings, once something is online it can be copied and redistributed and it is easy to lose control of the information. Work on the assumption that everything you post on line will be permanent and will be shared with others.
- **Take appropriate action if you are the target of abuse online**. If you find yourself the target of bullying or abuse online then you can take action in dealing with this, such as blocking individuals from interacting with you and using the sites' support mechanisms to report inappropriate activity. The United Learning Bullying and Harassment policy also sets out support mechanisms to deal with cyber bullying issues.
- **Be considerate to your colleagues**. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual concerned. Always remove information about a colleague if they ask you to do so.
- **Respect the privacy of other**s. If photographs are taken at a United Learning event then check whether those in attendance expect that any photos may appear on a public social networking site before posting. Remember it may not always be an appropriate way to share information whether work related or not.
- **Update any online sources in a transparent manner**. In the course of work, employees may find errors or out of date information displayed through online encyclopaedias. If updating this information then you must be transparent about who you are and the capacity in which you are doing this. Employees should consult with their line manager before updating or amending any information about United Learning from an on line source.
- **Remember the benefits**. Used responsibly, social networking sites can be accessed to keep up to date with a number of professions and information. Many use Facebook, Twitter and Linkedin to update and communicate with members. Work blogs may also be useful for communication, networking and professional development purposes but must be discussed and agreed with your relevant Manager.

DO NOT

- **Share confidential information online**. In line with the Data Protection Act 1998 employees should not share any child / young person / mother / father / carer identifiable information online or any personal information about colleagues. In addition to this, any confidential information about United Learning should not be revealed online.
- **Build or pursue relationships with children, young people, mothers and fathers / carers**. Even if the child / young person / mother / father / carer is no longer within your care, United Learning does not deem this as appropriate behaviour. If you receive a request from a child / young person / mother / father / carer / then many sites allow you to ignore this request without the individual being informed to avoid any offence. If you are concerned about this in any circumstance, please discuss with your Line Manager.
- **Use social networking sites to inform professional practice**. There are some circumstances/ job roles where this may be appropriate however careful consideration and discussions with management should be applied in line with the information set out in section 5.5 of this policy.
- **Discuss work related issues online**. This takes into account conversations about child / young person / mother / father / carer / colleagues or anything else which may identify United Learning online and bring it into potential disrepute. Even if you think these conversations have been anonymised they are very likely to be deemed inappropriate.
- **Post pictures of children/young people/their mothers/fathers/carers**. Never post pictures online even if they have asked you to do this. Employees should never take pictures of a child / young person / mother / father / carer unless they are relevant. If your mobile phone has a camera then this should not be used in the workplace.
- **Raise concerns about your work**. Social networking sites should never be used for raising or escalating concerns at work. If you have concerns then these should be raised through either discussing with your line manager or following United Learning's policy/procedure for raising concerns at work.
- **Engage in activities online which may bring the Organisation into disrepute**. Think through what activities you take part in whilst online and what you do or say that may bring United Learning into disrepute. Any reports of this will be reviewed in line with their appropriateness.
- **Be abusive to or bully other colleagues**. Social networking sites should not be used as a forum for abusive behaviour towards colleagues.
- **Post derogatory, defamatory or offensive comments** about colleagues, the children / young person / mothers / fathers / carers, your work or Rowan Preparatory School. Everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate comments.
- All of the above applies to both open and private sections of any social networking site with which employees identify themselves.

Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Key Personnel

The Headmistress is responsible for reviewing and authorising the policy.

United Learning Technology department via the Technology Business Partner can provide educational and technical expertise on Internet filtering.

Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by the IT & Facilities Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- Be reviewed with the DSL if significant changes are requested
- be reported to the E-Safety Group every term through a review of the system audit trail of changes made

A log of suspicious searches is created and sent to the DSL to identify any causes for concern to be followed up.

All users have a responsibility to report immediately to IT & Facilities Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Any breach of the filtering policy will result in action in line with the United Learning Disciplinary Policy
- The school has provided enhanced / differentiated user-level filtering through the use of the Lightspeed Filtering programme
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headmistress

- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the IT & Facilities Manager, Ian Jackson. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT & Facilities Manager who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the E safety Group

Records of reviews of usage of the school network and the Internet will be made available to the E safety group.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Technical Security Policy (including passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Key Personnel

The Senior Leadership team are responsible for reviewing this policy, along with the E safety Governor.

Advice on Technical Security can be obtained from the United Learning technology department through the technology business partner.

Responsibilities

The management of technical security is be the responsibility of the IT & Facilities Manager.

Technical Security

Policy statements

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. Guidance and training will be provided to ensure staff involve are effective in carrying out their responsibilities.

There will be regular reviews of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriately trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT & Facilities Manager and will be reviewed, at least annually, by the E-Safety Committee.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The IT & Facilities Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile device security and management procedures are in place.
- The IT & Facilities Manager regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by the IT & Facilities Manager to control workstations and view users activity
- Any actual / potential technical incident should be reported to the IT & Facilities Manager for investigation.
- An agreed process is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system. Rowan has generic logon account which enables supply teacher's access to school shared resources and also filtered Internet Access.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users. This is covered in the 'Rowan Acceptable use of ICT Staff' document with the section titled **'Software'.**
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school. At Rowan this is incorporated in the documents titled; Rowan iPad Agreement, Rowan Mobile Device Agreement.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. This is included in the 'Rowan Acceptable use of ICT Staff' document with the titles sections; **'Security of Information'** and '**Laptops/ IPADs and Portable Storage Devices'**
- An agreed policy is in place regarding staff use of own personal devices to access school systems and data to ensure suitable security solutions are in place to protect data.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans, etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. A secure file transfer mechanism is available for sharing data with other organisations working with the school.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT & Facilities Manager and will be reviewed, at least annually, by the E-Safety Committee .
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headmistress and Business Manager and kept in a secure place e.g. school safe.
- Passwords for new users, and replacement passwords for existing users will be allocated by the IT & Facilities Managers
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below

- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account

Staff passwords:

- All staff users will be provided with a username and password by the IT & Facilities Manager who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed
- should be changed at least every 60 to 90 days
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised

Pupil passwords

- For pupils in KS1 and EYFS class log in details will be set up by the IT & Facilities Manager and issued to the class teacher. Strict access controls are in place for content for this group of pupils.
- All pupil users in KS2 will be provided with a username and password by the IT & Facilities Manager who will keep an up to date record of users and their usernames.
- KS2 users will be required to set a password which will remain for their time at Rowan unless a change is requested via SLT. Strict access controls are in place for content for this group of pupils.
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The IT & Facilities Manager will ensure that full records are kept of:

- User Ids and password changes
- User log-ons
- Security incidents related to this policy

Relevant Legislation

Schools should be aware of the United Learning Policies and legislative framework under which this guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

United Learning Policies

- Child Protection Policy
- Safeguarding Policy
- Disciplinary Policy
- Bullying and Harassment Policy
- Whistleblowing Policy

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of an individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
  - Ascertain whether the communication is business or personal;
  - Protect or support helpline staff.
- The organisation reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. Youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes 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.

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.

Protection of Children Act 1978

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 a 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

Sexual Offences Act 2003

The offence of grooming 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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of work with young people, human rights to be aware of include:

- The right to a fair trial

- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The organisation is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

UK GDPR

This protects the rights and privacy of an individual's data and provides harmonisation of data protection law across the UK.

It defines the obligations of data controllers and data processors to keep records of data processing including the legal basis for collecting data, the purpose for which it is used, how long it is retained, how it is kept secure.

Defines the rights of the data subject to be informed, have access, to rectification of errors and erasure and to portability.

Links to other organisations or documents

UK Safer Internet Centre

- Safer Internet Centre -
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others:

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
- Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

- Specialist help and support SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government Better relationships, better learning, better behaviour
- DCSF - Cyberbullying guidance
- DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

- Digizen – Social Networking
- SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- SWGfL Digital Literacy & Citizenship curriculum
- Glow - http://www.educationscotland.gov.uk/usingglowandict/
- Alberta, Canada - digital citizenship policy development guide.pdf
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Somerset - e-Sense materials for schools

Mobile Devices / BYOD

- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN - Guidance Note - BYOD

Data Protection

- Information Commissioners Office:
    - Your rights to your information – Resources for Schools - ICO
    - ICO pages for young people
    - Guide to Data Protection Act - Information Commissioners Office
    - Guide to the Freedom of Information Act - Information Commissioners Office
    - ICO guidance on the Freedom of Information Model Publication Scheme
    - ICO Freedom of Information Model Publication Scheme Template for schools (England)
    - ICO - Guidance we gave to schools - September 2012 (England)
    - ICO Guidance on Bring Your Own Device
    - ICO Guidance on Cloud Hosted Services
    - Information Commissioners Office good practice note on taking photos in schools
    - ICO Guidance Data Protection Practical Guide to IT Security
    - ICO – Think Privacy Toolkit
    - ICO – Personal Information Online – Code of Practice
    - ICO – Access Aware Toolkit
    - ICO Subject Access Code of Practice
    - ICO – Guidance on Data Security Breach Management
- SWGfL - Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- Somerset - Flowchart on Storage of Personal Data
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Kent - Safer Practice with Technology
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Note - esecurity

Working with parents and carers

- SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum
- SWGfL BOOST Presentations - parents presentation
- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- DirectGov - Internet Safety for parents
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops / education

- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- The Cybersmile Foundation (cyberbullying) - advice for parents

Research

- EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
- Futurelab - "Digital participation - its not chalk and talk any more!"

Rowan Preparatory School

Acceptable Usage of Technology (AUP) for Pupils and Parents

Policy Statement: Rowan Preparatory School has a responsibility to ensure that each pupil is kept safe when using all aspects of Computing. This includes that the provision of Computing is being used appropriately and that any technologies brought onto the school site by individual students do not pose a threat to others and do not bring the school into disrepute.

It is the duty of our school to ensure that every pupil in our care is safe and this applies to the virtual or digital world of the Internet as much as it does to the physical environment of the school.

Both Pupils and Parents are asked to indicate that the Acceptable Use and E-Safety Rules have been understood and agreed. This is an agreement to run throughout the pupil's education at Rowan Preparatory School.

Rules of acceptable use of all Computing at Rowan Preparatory School

Use of Computing resources provided by the school:

- The computer system is available for educational use only.
- I will only log on with my own username and password.
- I will not share my username and password with anyone else.
- I understand that the school monitors the use of the information systems.
- I will make sure my work is finished and checked before I print it and only print when instructed to do so.
- I will take care when using the equipment so as to not cause damage.
- I understand that all internet and network usage is logged and this information may be made available to my parents.
- If I do not follow these rules, then I understand that there will be a consequence.

The rules help us to stay safe on the Internet:

- I ask permission before using the Internet.
- I only use websites that an adult has chosen or helped me to choose.
- I tell an adult immediately if I see or read anything I am uncomfortable with and switch my screen off.
- I only use the internet if an adult is in the room with me.
- I only email people an adult has approved.
- I send emails that are polite and friendly.
- I never give out personal information about myself or others, including any passwords.
- I never arrange to meet anyone I do not know.
- I do not open emails sent by anyone I do not know.
- I do not use Internet chat rooms.
- I am not allowed to connect personal devices to the school network.

- If I have permission to travel to school independently, I will leave my mobile phone with the office during the school day.
- I will only post content online if it appropriate and I have permission.

Acceptable Use of Technology
Pupil and Parent Agreement Form

I have read all the points relating to acceptable use of COMPUTING resources and agree to abide by those terms and conditions.

Pupil signature .... Date…………………………………………

I have spoken to my daughter about acceptable use of Computing and I agree that they may use the school Computing facilities and internet in accordance with the school rules regarding acceptable use.

E-Safety includes helping children to stay safe while using all modern digital media and devices, including email, mobile phones, chat-rooms, social networking etc.

We recommend that all parents of primary age children take time to discuss these issues with their child on an ongoing basis.

The Child Exploitation and Online Protection website is the government's official resource to assist both teachers and parents in explaining to children the benefits and risks associated with digital media. It is a good place to start when tackling this important subject. www.thinkuknow.com

Parent signature……………………………………….. Date…………………………………………

This policy applies to all members of our school community, including those in our EYFS setting.
Rowan Preparatory School is fully committed to ensuring that the application of this Pupil & Parent Acceptable Use policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.
Rowan Preparatory School seeks to implement this policy through adherence to the procedures set out in the rest of this document.
*This document is available to all interested parties on our website and internal Rowan Network Shared Areas and should be read in conjunction with the E-*Safety Policy.

This document is reviewed annually by Vicky Langham – Business Manager, or as events or legislation change requires. The next scheduled date for review is November 2024..

Mobile Device Guidelines for Pupils

Rowan Preparatory School discourages pupils from bringing personal mobile technology devices to school. This includes mobile phones, smart phones, iPads, tablets and laptops.

- If a pupil needs to bring a mobile device to school, for example if they walk home, parents are asked to notify the school in writing.
- When a mobile device is brought into school it must be clearly labelled with the pupil's name. It must remain switched off and given in to the school office on arrival at school.
- The mobile device must be collected at the end of the school day form the school office and must not be switched on until leaving the site.
- Pupils must not take personal mobile devices on school trips as a substitute for a camera.
- Where a pupil is found with a mobile device in school, including in the playground, the device will be taken from the pupil and placed in the office. Parents will be contacted to collect it at the end of the day.
- If a pupil is found taking photographs or video footage with a personal mobile device of either pupils or teachers this will be regarded as a serious offence. The Headmistress will decide on appropriate disciplinary action.
- Parents are advised that Rowan Preparatory School accepts no liability for loss or damage to any mobile devices that are brought into school.

This policy applies to all members of our school community, including those in our EYFS setting.
Rowan Preparatory School is fully committed to ensuring that the application of this Pupil & Parent Acceptable Use policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.
Rowan Preparatory School seeks to implement this policy through adherence to the procedures set out in the rest of this document.
This document is available to all interested parties on our website and internal Rowan Network Shared Areas and should be read in conjunction with the E-Safety Policy.

This document is reviewed annually by Vicky Langham – Business Manager, or as events or legislation change requires. The next scheduled date for review is November 2024..

- **Pupil Acceptable Use of Technology**
- **Additional points when working from home**
- **Note to parents**

Girls are expected to read and discuss these additions to the Pupil Acceptable Use of Technology agreement with you and then to follow the terms of this policy.

If you have any concerns or queries please email your daughter's form teacher.

Please note that Rowan Preparatory School will not be able to provide technical IT support beyond ensuring that log on details work correctly. Specific guidelines on use of the various applications to be used by each year group will be communicated separately.

Please support your daughter's online learning in the following ways:

- Provide a WiFi enabled workspace that is quiet and free from distractions with an adult nearby to safeguard them.

- Ensure that girls are dressed appropriately for engaging in education if it is interactive.

- Ensure that face to face communication is only between teachers and pupil, similar to in a classroom. Any parent pupil communication should be in the usual manner via email.

- Not recording, sharing or commenting on public forums about individual teachers.

- Ensuring your daughter ends any online interactive session as soon as the teacher indicates to do so.

Please complete the form below to acknowledge that you have read this communication and policy and reviewed it with your daughter. Please also confirm that you give permission for your daughter to participate in online interactive sessions with the teachers from Rowan Preparatory School. These sessions may be recorded.

- I have read this communication regarding Acceptable Use of Technology by pupils when working at home*

□ Yes

- I have reviewed this policy with my daughter*

□ Yes

- I give permission for my daughter to participate in online interactive sessions with the teachers from Rowan Preparatory School and agree to the sessions being recorded.*

□ Yes

- Name of person completing form*

________ First Name ________ Last Name

Rowan Preparatory School

Acceptable Usage of Technology for Staff (including temporary staff and visitors)

Policy Statement: The following conditions cover the use of all Information and Communication Technologies in school and when connected to the Rowan Network externally, including email, internet, network access and shared areas, software, equipment, telephone systems and the school website.

Security of Information
Confidential data (e.g. student/staff personal data, financial information and management data) must not be transported between home and school using any form of removable storage media, but should be accessed either at school, through the School Information system (iSAMS) or when accessing the Rowan Network from home.
The data protection policy requires that any information with regard to staff or student and/or held within the school's management information system, will be kept private and confidential, except when it is deemed necessary to disclose such information to an appropriate authority.
Data belonging to the school or United Learning must not be transferred outside of the organisations' systems except via Group email or encrypted media. This includes use of cloud storage which has not been verified as secure by the IT & Facilities Manager (Ian Jackson) or Central Office IT Services.

Passwords
Password(s) should be kept secret, must not be shared with others and should be changed on a regular basis (or when directed to do so).

Email
All business related emails should be sent via the school's email system. Personal email accounts must not be used. All emails sent externally must be professional in their approach, just as any letter sent out is written in a professional manner, as these reflect the image of the school.

Internet
Internet filtering is in place which prevents access to unsuitable websites. However, pupils must still be supervised at all times. Unblocking of sites must be requested to the IT & Facilities Manager (Ian Jackson), but may be declined if deemed inappropriate.

Social Networking Websites *'Social Networking' refers to any website or digital resource designed to facilitate social interaction between people in either private or public online spaces.*

Staff must ensure that any private social networking sites/blogs, etc that they create or actively contribute to are not confused with their professional role. It is professionally inappropriate for staff to have current pupils as contacts/friends on such systems. Staff must not use social networking sites to contact or communicate with pupils or those who have recently left. Staff must not view pupils' social networking pages. Staff must report any inappropriate material posted on a social network about themselves, Rowan School, or a pupil, to the Senior Leadership Team.

Security of Equipment
No portable ICT equipment should be left unguarded in classrooms, staffroom, offices or other areas of the school. They should be stored in cupboards or drawers when not in use. Laptops /IPADs and other mobile devices

should not be left in vehicles, even in the boot. If loaned equipment is mislaid the cost of replacement may be charged to the department it was loaned to.

Back-up Arrangements
All Staff who use ICT as part of their job are able to save their work onto the school server. The server is backed up on a daily basis.

Network Access from Home – please see use of own devices policy
Unauthorised individuals must not be allowed to access Rowan email/internet/network, or other school third-party systems on your behalf. You must not allow friends or family members to use your Laptop/PC whilst you are connected to the Rowan Network or Rowan email systems. Likewise, you must not leave your Laptop/PC unattended whilst connected to the Rowan Network or Rowan email.

Mobile Devices – Personal and school owned
Guidelines for use of Mobile devices are published for staff to follow. These include both personally owned devices and those provided by school. School provided iPADs, Smartphones and Laptops are issued with a usage agreement document.

Data Storage & Data Transfer
Work should be stored within the secure school network and not on local drives on desktop computers or mobile devices. This provides both security against unauthorised access and back up of data for contingency purposes.
If work is stored for short periods of time on mobile devices including memory sticks the devices should have a level of security in place such as password control or encryption and be deleted as soon as possible form these devices. This is particularly important for any data deemed to be Personal data i.e. information that relates to an identifiable person.

If data is required to be shared outside the school for bona fide purposes extreme care must be taken if it is deemed to be Personal data i.e. information that relates to an identifiable person. Files should only be transferred with an appropriate level of security in place eg. Password control, encryption and preferably a secure file transfer mechanism should be used. For advice relating to the contact the IT & Facilities Manager.

Virus Protection
The school provides appropriate virus protection for all school computers, laptops and servers.

Software
It is the policy of the school to respect all computer software copyrights and to adhere to the terms of all software licences. It is the legal obligation of the school and its employees to comply with copyright laws and respect the intellectual property rights of others. It is therefore expressly forbidden for any employee to have possession of unlicensed software on school premises or use unlicensed software on school computers. Users may not duplicate any licensed software or related documentation unless expressly authorised to do so by agreement with the licenser. Unauthorised duplication of software may subject users and/or the school to both civil and criminal penalties under the Copyright Designs and Patents Act 1988 (and related EC directives). To purchase software, users must obtain the approval of the IT & Facilities Manager (Ian Jackson), who is also responsible for registering software with the software publisher and maintaining a register of all software used in school. According to the Copyright, Designs and patents Act 1988, infringement of software is actionable in the civil courts. Users who make, acquire or use unauthorised copies of software will be disciplined as appropriate under the circumstances.

Hardware
All ICT hardware must be purchased through the IT & Facilities Manager (Ian Jackson) in order to ensure that an up-to-date ICT asset register is maintained for the school. Deliveries should be checked by the IT & Facilities Manager and appropriate set up arrangements installed where necessary before being given to the member of staff who requested the item. All new ICT hardware must have its serial number logged and added to the school's inventory.

Health & Safety
Staff should be aware of Health & Safety guidance relating to regular use of technology and should complete a Display Screen Assessment questionnaire if a frequent and regular user to assist in determining any specific support or adjustment required in the workplace.

Use of Computing in school
When using computing and communication facilities provided by the school the following rules apply:

- The school's Computing resources and communication systems may only be used for professional purposes or for uses deemed "reasonable" by the Headmistress and United Learning.

- During registration and lesson time (including PPA) teaching staff may only use ICT for appropriate school-related work.

- Computing and communication facilities, including telephones, may be used for reasonable personal use outside of core working hours. Such use is permitted during break times and lunch times. However, priority must be given to those members of staff wishing to use computers and telephones for school business.

- Browsing, downloading, accessing or sending material that could be considered offensive to others, including materials classified as pornography, profanity, criminal skills, hate and extreme, is not permitted at any time.

- Reasonable use of the school's telephone system excludes making international calls (except where explicit permission has been given) and using premium rate services or services which could be considered offensive to others.

- The school's approved email system must be used for all school business except in exceptional circumstances (e.g. critical incident which leads to a loss of school systems).

- Only the approved school email system, Clarion Call Parent messaging and Parent Portal or other school-approved communication systems must be used when communicating with students or parents/carers, and communication with them must be on appropriate school business.

- Downloading software or resources from the internet which could compromise the school's IT system or which could be subject to licensing must only be done through the IT & Facilities Manager.

- Staff should not attempt to connect any device to the school network without the permission of the IT & Facilities Manager (Ian Jackson).

- Personal digital cameras or camera phones should not be used for taking and transferring images of students or staff and the storage of images at home is not permitted. If a school camera is used for this purpose the pictures must be downloaded onto the school network and the images should then be deleted from that camera.

Use of school-provided ICT resources at home/ from outside school

- Any computer, laptop, IPAD or other mobile device loaned to a member of staff by the school, is provided solely to support their professional responsibilities and that all terms of acceptable use outlined in this policy apply to the use of the loan equipment. Staff are required to sign an additional loan agreement document setting out the terms of use.

- Any computing device loaned to staff members must be returned on request to the IT & Facilities Manager so that any anti-virus, security, software upgrades or hardware upgrades can be installed or maintained.

- All terms relating to acceptable use of technology apply when accessing the Rowan Network, email or school information system (iSAMS) from home / outside school

- As per the school's Data Security Policy, school data must not be downloaded to personal computers or laptops and staff should not leave personal computers connected to school systems unattended or allow other individuals to use such systems.

Use of personally owned devices to access school and United Learning data

- Under GDPR (General Data Protection Regulations) United Learning including Rowan Preparatory School must remain in control of the data for which it is responsible, process this lawfully and keep it for no longer than necessary. This obligation exists regardless of the device used.

- You may choose at times to access emails and school and/or United Learning data from your own personal devices including mobile phone, iPAD, PC /Mac. This is permissible provided that you have read and comply with the policy for accessing data using your own device. This policy provides clear guidance regarding security processes and registration of your device.

- Should you wish to use your own device(s) please contact the Network Manager/ IT technician to obtain a copy of the policy and arrange completion of the relevant security checklist.

- *This policy applies to all members of our school community, including those in our EYFS setting.*

- *Rowan Preparatory School is fully committed to ensuring that the application of this Staff Acceptable Use policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.*

- *Rowan Preparatory School seeks to implement this policy through adherence to the procedures set out in the rest of this document.*

- *This document is available to all interested parties on our website and internal Rowan Network Shared Areas and should be read in conjunction with the E*-Safety Policy.

- *This document is reviewed annually by Vicky Langham – Business Manager, or as events or legislation change requires. The next scheduled date for review is November 2024.*

Mobile Device Guidelines for Staff

Staff personal mobile digital devices

1) Staff personal mobile digital devices should be switched off (or in silent mode) during lessons, or at times where they are responsible for the supervision of students.
2) Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to receive or send personal calls, texts or post content to personal social media platforms.
3) If a member of staff feels that it is necessary to be available to receive a personal call or text on a personal mobile device during a lesson, for which there may be exceptional circumstances, they should explain this to their line manager beforehand.
4) Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to access online resources, emails, apps or similar, unless it is considered that the outcome is essential to pupil learning and cannot be sourced through the school network (in which case, pupils should be made aware that the mobile device has been used for this educational purpose).
5) Staff must not photograph or video pupils with a personal (mobile digital) device. If it is necessary to regularly take images of students for marketing purposes, then a school owned device should be provided.
6) Staff should endeavour to make any personal calls on their own mobile telephone, or similar, in a discreet fashion and away from any pupil area, for example in the Staff Room or in an office, behind closed doors.
7) Staff should not give out their personal mobile phone numbers, or other communication contact information, to students.

Inappropriate use of mobile devices is a serious offence; cases of misuse could lead to disciplinary action being taken against the individual concerned.

School owned mobile digital devices

When school owned mobile devices (IPADS or mobile phones) are issued to staff they are asked to read and sign a loan agreement setting out the Acceptable of use of school equipment. The “Rowan iPad Agreement” is included as an appendix.

- Equipment issued to staff remains the property of Rowan Preparatory School and is loaned for the duration of your employment or until a request is made for its return.
- Individual staff members are the designated user of the iPad, identified by its serial number and the label affixed to the front of the iPad of which must not be removed.
- The iPad is connected to the staff members school email account and therefore may have access to the personal information of pupils. Staff are made aware that this means they must be fully comply with Rowan Preparatory Schools’ data protection policy.
- Staff must inform Ian Jackson (IT & Facilities Manager) or a member of SLT as soon as possible if the iPad is lost or stolen.
- The iPad may be ‘remotely wiped’ (all content deleted) by Rowan Preparatory School if the content on the iPad is thought to be in jeopardy by the iPad being lost or stolen.

- The school will provide a standard collection of apps for use on the iPad. In addition it may provide some specific apps related to a specific role or department. These apps must not be deleted from the iPad at any time and any non-work related apps for personal use should not be installed.
- Staff must take all reasonable precautions to protect the content on the iPad and a passcode must be enabled at all times.
- Any personal content on the iPad must not breach the Rowan ICT Acceptable Use Policy.
- The school may request the return of the iPad at any time without notice for inspection purposes.
- The iPad must be enclosed in its designated case at all times.
- When a member of staff leaves the employment of Rowan Preparatory School, the iPad, case and charger must be returned to Ian Jackson (IT & Facilities Manager) before you leave.
- Photographs or video of pupils are prohibited on iPad devices that are taken off-site e.g. taken home.
- Photographs or video of pupils for the purposes of Teaching and Assessment may be allowed provided that:
    - The iPad is based permanently in school.
    - The activity complies with the school's Child Protection, e-Safety, ICT Acceptable Use and Health and Safety Policies.
    - The photos/videos are not stored on the iPad for an extended period beyond the time required for their use.
    - That the photos/videos are only backed up to the school network system.
- IPads are checked occasionally for updates and for compliance with school policies. Outcomes will be reported to the Headmistress or Business Manager. Breaches of the agreement may result in the school requesting the return of the allocated iPad and further disciplinary action being taken.

Use of mobile devices: guidelines for staff use (photographs and videos)

Staff working in the EYFS setting are specifically prohibited by EYFS regulations from using their personal devices (cameras, mobile phones, IPADS) to take photographs or videos of children in the EYFS setting for any reason. Only school devices may be used. Rowan has decided to extend this to be policy throughout the school.

Staff must under no circumstances ever use any photographs of students for anything other than strictly professional purposes. They must never upload photographs or videos of any students onto the internet or social media site. The only exception is for the marketing department to use photographs of students, where parents have given consent, on the school’s own website or other school managed social media platforms.

After taking photographs of students on mobile devices, staff should not store these for any longer than necessary, and once copied onto the school network should be deleted from the mobile devices.

Before printing any photographs of students in any external publication (e.g. local or national newspapers), parents must give permission for the student’s photograph and/or name to be used.

ROWAN
PREPARATORY
SCHOOL
1936
HIC FELICITER LABORAMUS

Acceptable Use of ICT
Staff Agreement Form
2024/25

I have read the Staff Acceptable use of Technology policy, understand it and intend to comply with its obligations.

I have read the Guidelines for Staff on Use of Mobile Devices and agree to abide by these.

I understand that usage of school ICT systems is logged and this information will be made available to the Headmistress on request.

I understand that prior to using my own devices to access company systems I must read and follow the school policy for this. This includes completion of a questionnaire relating to the device(s) I will be using and review of this with the Network manager.

I understand that failure to comply with this agreement regarding use of IT could lead to disciplinary action.

Signature: ………………………………………………… Date: ………………..

Full Name: …………………………………………………….……. (printed)

Job Title: ....

Completed form to be returned to the Business Manager, Vicky Langham, for filing with HR records.

Policy for Accessing United Learning Data Using your Own Device

Scope

The policy and procedure set out in this document applies to all United Church Schools Trust (UCST) and United Learning Trust (ULT) staff; including fixed-term, part-time, full-time, permanent and temporary staff.
Where this policy refers to 'School' or 'Head Teacher' within Central Office this should be interpreted to refer to the department where a member of staff works and their Head of Department.

UCST and ULT are registered charities and form part of the trading name, United Learning. As a values-led organisation, our values of ambition, confidence, creativity, respect, enthusiasm and determination are key to our purpose and underpin all that we do.

1. Introduction

1.1. Under GPDR, United Learning must remain in control of the corporate data for which it is responsible, process it lawfully and keep it for no longer than is necessary. This obligation exists regardless of the ownership of the device used to carry out the data processing or storage. For example, if you were to use your own device to access your United Learning email account, United Learning needs to ensure that those emails (and any attachments, etc.) do not leave its control. As an employee, you are required to play a role in keeping your United Learning data secure. Your attention is also drawn to your IT Acceptable Usage Policy which requires you as an individual to process data in compliance with all aspects of the GDPR and this applies equally to processing of data which takes place in the context of BYOD.

1.2. This policy is intended to provide a clear framework for the secure use of personal devices in the workplace. By personal devices, it is meant smart phones, tablets, laptops and home computers that belong to the employee but which are used for work purposes as well as for private use. This is commonly known as '**Bring Your Own Device**' (BYOD).

1.3. This policy also aims to provide guidelines for staff to access their Microsoft Office 365 accounts through a browser, without undertaking the full BYOD process.

1.4. The policy aims to find a balance between the convenience that BYOD offers and the security of United Learning data and the integrity of our systems.

1.5. As an employee, you are also required to assist United Learning in complying with Subject Access Requests and other requests made under the Freedom of Information Act, which may include data stored on a personal device if it is being used for work purposes.

1.6. Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action under United Learning's disciplinary policy.

2. What are the benefits of BYOD?

2.1. Some people prefer to use their personal device for reasons of ergonomics, convenience, efficiency and Operating System preferences.

2.2. United Learning’s licensing for its Anti-Virus software and for Microsoft Office can be extended to cover your personal devices. Office 365 enables remote workers to work ‘just in the browser’ eliminating the need for local copies of any data.

3. General principles for keeping data secure

3.1. Data must at all times remain within United Learning systems – emails must not be forwarded to private accounts (e.g. Gmail, Hotmail etc) and files should only be stored within OneDrive rather than saved locally (to the desktop or C drive for example).

3.2. Transferring data out of United Learning systems for use elsewhere using removable media (USB sticks, DVDs) or non-approved cloud storage services (Dropbox, Google Drive, etc.) is not permitted. Doing so heightens the risk that data will leave United Learning’s control.

3.3. Do not engage in risky activities using the BYOD device in your private life. For example, visiting websites with gambling, adult or illegal content would place the device at greater risk of malware.

3.4. You must not allow any non-employee of United Learning to access your device (including family members). This is an important consideration when deciding whether you wish to use your own device for work. This is especially true of mobile phones and tablets where it is unlikely that separate accounts can be set up. Family use of Windows PCs/ Macs is allowed as long as separate accounts are set up, the account being used for work is completely separate, account details are not to be shared and passwords meet the complexity levels above. Other accounts on the device must not be ‘Admin’ type accounts that grant access to other areas of the device.

3.5. You must not attempt to connect your device to your United Learning networks except guest networks. Your local IT Help Desk can assist with this if necessary.

3.6. Devices must not be jailbroken, rooted or have any software/firmware installed designed to allow access to unofficial applications. This weakens the device’s security.

4. What do you need to do if you want to BYOD?

4.1. Refer to the BYOD policy and guidance above, ensuring you complete the correct checklist relevant to your device (see below). Your local IT help desk staff can support you & ensure checklist requirements are in place.

4.2. Submit the signed policy and relevant checklists to your line manager for approval.

I only want to read emails, check my calendar, or access other United Learning or school data from within a web browser and never download data to my device.
Go to:-

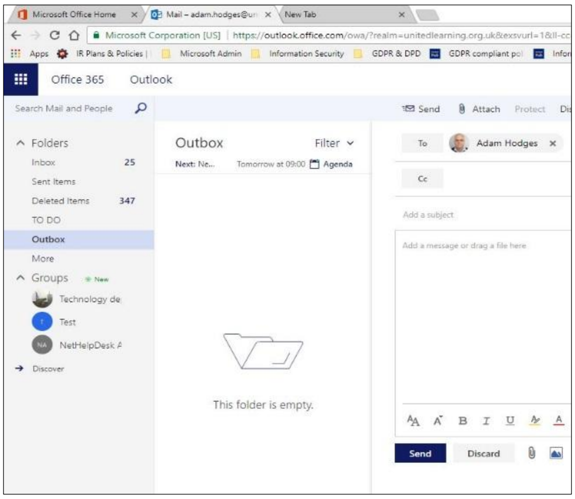
Section A (browser)

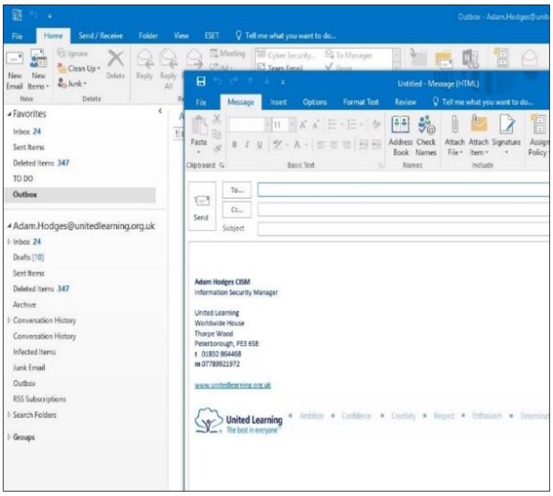
I want to download United Learning or school data to my device and work on these with the native/ desktop applications e.g. Mail for iPhone, Office 2016, Outlook.
Go to:-

Section B (BYOD)

For example:
Below an email has been composed within the latest version of Chrome. Provided that this is all done from within a browser then BYOD compliance is not needed as no personal data is stored on the device.

For example:
Below, the Outlook 2016 desktop application is being used to compose an email. For this scenario BYOD compliance is necessary as personal data is stored on the device.





Adam Hodges CISM
Information Security Manager

United Learning
Worldwide House
Thorpe Wood
Peterborough, PE3 6SB
t 01832 864468
m 07789921972

www.unitedlearning.org.uk

You must sign to Section A and/ or Section B, depending on how you will be accessing data and systems

SECTION A

1. Accessing data and systems through a browser

1.1. You will only access Microsoft O365 applications (Word, PowerPoint, Outlook, OneDrive, SharePoint etc) from within a current browser. Office 365 is designed to work with the current versions of Safari, Chrome, Edge

1.2. No documents, presentations, emails or other files will be downloaded to the device on which you are running the browser session. All work must be carried out within the browser-based versions of Office 365 tools (Outlook, Word, etc). Do not use the OneDrive sync client as it stores a copy of your files locally.

1.3. The device will have a current & supported Operating System and be kept up-to-date with patches.

1.4. For Windows and OSX devices, a commercial and up-to-date anti-virus program must be installed.

1.5. School/ United Learning passwords must not be stored (saved) on the device, and do not select the option to stay 'logged in'.

1.6. In the event that the device is lost/stolen/sold/returned to the manufacturer or vendor, you will change your United Learning system passwords.

1.7. Accessing your United Learning Office 365 account from an internet café (or similar) is not permitted, unless in the event of exceptional circumstances. If abroad, it will always be safer to use your own phone/ tablet on your hotel's Wi-Fi than to entrust your credentials to a shared computer in an Internet cafe.

Signature:……………………………………………………………………………………………

Print name:…………………………………………………………………………………………..

Section B

1. **You agree:-**
    1.1. that your device will comply with the relevant checklist below, ensuring that:
    1.2. Operating Systems are supported and up-to-date
    1.3. Suitable virus protection is in place
    1.4. Hard drives are encrypted
    1.5. Device access security is in place

2. **What are the implications for employees who want to use their own device(s) under this policy?**
    2.1. Your device must use one of the Operating Systems and versions listed in Appendix 1
    2.2. Devices (where they reasonably can be) should be encrypted. You are strongly advised to read the advice below (see Frequently Asked Questions) on encryption and recovery keys.
    2.3. You must agree to install a satisfactory anti-virus program on the BYOD devices.
    2.4. You must agree to keep your device up to date with the latest operating system patches and other software (e.g. Microsoft Office). Software companies regularly patch their products to protect users against emergent threats and exploits which have been discovered and unpatched devices are especially vulnerable. In summary – keep your device up to date.
    2.5. You must agree to protect your device via a complex password (8 characters or greater, including at least one of the following - numbers, upper and lower case letters) or a biometric measure. Please see here for the United Learning Password Policy.
    2.6. You must set up any mobile device (phone, tablet, and laptop) to auto-lock after a set period of idleness – a maximum of 5 minutes is suggested.
    2.7. In the eventuality that your device is lost, stolen, destroyed, returned to the manufacturer, becomes end-of-life or stops being used by you for work, you must inform your IT Help Desk and immediately change all passwords related to your access to United Learning systems.
    2.8. You must keep any personal data separate from United Learning data. The simplest way to achieve this is to use the OneDrive client which your IT Help Desk will set up for you.
    2.9. You must agree to co-operate with officers of United Learning when they consider it necessary to access or inspect corporate data stored on your device.
    2.10. You must agree that United Learning is not liable for any costs relating to your device, including but not limited to: purchase, insurance, licensing, contract costs, call charges, repairs and peripherals/ accessories.
    2.11. You must agree that United Learning may at any point and without consultation rescind the right to use your device to access its systems and data.
    2.12. You must agree that the IT Help Desk is not responsible for supporting your use of this device beyond initial set up of United Learning systems and ongoing help to use these systems.
    2.13. United Learning will monitor the devices connecting to its networks and reserves the right to prevent access for any device that is considered a risk to the network's integrity and security.

United Learning will not monitor private usage of the device. In exceptional circumstances, United Learning may require access to corporate data stored on your personal device. In those circumstances, every effort will be made to ensure that a United Learning employee does not access the private information of the individual.

Your local school/ centre will maintain a register of devices used by employees under this policy.

BYOD Checklist - Computer or Laptop

Please ensure that you understand the risk associated with encrypting hard drives should the encryption key be lost.

1. Your name and line manager approval:

Employee Name	
Line manager approval	Signed by Click or tap here to enter text.

2. Now that you have authorisation to use your own device to for your United Learning School you need to complete and confirm items 1-7 below. ***The FAQ section offers guidance on how to set up your device.*** It will then need checked by the ICT Help Desk. These two steps could, with agreement, be done at the same time.

		Device Owner	Technician Check
1	What is the operating system on your personal device?		☐
2	Do you ensure that updates are regularly applied?	Choose an item.	☐
3	Is Anti-Virus installed?	Choose an item.	☐
	If so which Anti-Virus is installed?	Click or tap here to enter text.	☐
4	Is the device protected by a compliant password?	Choose an item.	☐
5	Is an auto lock enabled?	Choose an item.	☐
6	Does each user of the device have their own account? Does the applicant have the only Admin account	Choose an item.	☐
7	Is the device encrypted?	Choose an item.	☐
8	Has the process for reporting a lost device been explained?	Choose an item.	☐
9	Has the level of support been explained?	Choose an item.	☐
10	Has the register of devices been updated?	Enter Device Name.	☐

Signed by User: Click or tap here to enter text.

Signed by Technician: Click or tap here to enter text.

BYOD Checklist - Phone or Tablet

1. Your name and line manager approval:

Employee Name	Click or tap here to enter text.
Line manager approval	Signed by Click or tap here to enter text.

2. Now that you have authorisation to use your own device to store United Learning data you need to complete items 1-6 below. ***The FAQ section offers guidance on how to set up your device.*** It will then need checked by the IT Help Desk. These two steps could, with agreement, be done at the same time.

		Device Owner	Technician Check
1	What is the operating system on your personal device?	Choose an item.	☐
2	Are OS updates automatically applied?		
3	Is Anti-Virus installed?	Choose an item.	☐
	If so which Anti-Virus is installed?	Click or tap here to enter text.	☐
4	Is the device protected by a suitably complex and secure password or passcode?	Choose an item.	☐
5	Is an auto lock enabled after 5 minutes?	Choose an item.	☐
6	Device has encryption turned on?	Choose an item.	☐
7	Has the process for reporting a lost device been explained?	Choose an item.	☐
8	Has the level of support been explained?	Choose an item.	☐
9	Has the register of devices been updated?	Enter Device Name.	☐

Signed by User: Click or tap here to enter text. **Signed by Technician**: Click or tap here to enter text.

FAQ – Frequently Asked Questions

Q: How can I make sure my device is updating?

A: Windows PC: Follow the link - https://support.microsoft.com/en-gb/help/12373/windows-update-faq - and select "How do I keep my PC up to date?" which will explain how to do it for Windows 10 and Windows 8.1
Mac OSX: Follow the steps in this link - https://support.apple.com/en-gb/HT201541

Q: Where can I get Anti-Virus software?

A: Windows PC/ Mac OS: It is likely that your school's/ centre's anti-virus licence can be extended to cover your BYOD device. If you bank online it is likely that your bank will offer you free anti-virus software. Some broadband providers also offer it free of charge.
iOS devices: These do not currently need AV software due to Apple controlled App Store
Android devices: We recommend Sophos from the Play Store - https://play.google.com/store/apps/details?id=com.sophos.smsec. Please note it will have an impact on battery life as it scans applications and files.

Q: How do I password protect my device?

A: All devices must have a password/passcode to make it harder to access data if it is lost or stolen. Remember not to lose it or share it with anyone else:
Windows 8.1 PC: follow the advice here - https://support.microsoft.com/en-us/help/13951/windows-create-user-account
Windows 10 PC: follow the advice here - https://support.microsoft.com/en-us/instantanswers/5de907f1-f8ba-4fd9-a89d-efd23fee918c/create-a-local-user-account-in-windows-10
Mac OSX: follow the advice here - https://support.apple.com/en-gb/HT202860
Apple Devices: - https://support.apple.com/en-us/HT204060
Android Devices: - http://www.itproportal.com/2015/04/28/how-to-set-up-passcode-android-ios/
https://www.howtogeek.com/253101/how-to-secure-your-android-phone-with-a-pin-password-or-pattern/

Q: How can I lock my screen?

A: For Windows: Follow the link https://support.microsoft.com/en-us/help/17185 - about personalising your lock screen. Alternatively you can alter your screensaver settings https://support.microsoft.com/en-us/instantanswers/166a4a91-2fc5-42a5-853b-024397ebfa74/change-your-screen-saver-settings
For OSX: Follow this link - https://support.apple.com/en-gb/HT204379

Q: How can I create accounts for each user on my PC or Mac?

In order to password protect your PC or Mac you will need to create user accounts for each person who uses it
A: Windows 8.1 PC: follow the advice here - https://support.microsoft.com/en-us/help/13951/windows-create-user-account
Windows 10 PC: follow the advice here - https://support.microsoft.com/en-us/instantanswers/5de907f1-f8ba-4fd9-a89d-efd23fee918c/create-a-local-user-account-in-windows-10
Mac OSX: follow the advice here - https://support.apple.com/en-gb/HT202860

Q: How do I encrypt my home PC or Mac Computer?

A: For Windows: This needs to be facilitated by your school/ centre's IT helpdesk.

For Mac: Turn on FileVault which is built in to every new Mac Operating System - https://support.apple.com/en-gb/HT204837

Q: Why do I need to encrypt my device?

A: Encrypting the device will prevent someone, who does not know the encryption key, from accessing data on the device should it leave your control in the future.

Q: How do I encrypt my home mobile device?

A: iPhone or iPad: enabling a passcode automatically encrypts it.
Android device: follow the advice in your phone manual or check the link here. Your device encryption might already be enabled by default. https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/

Q: How do I report the loss of my device?

A: In the first instance, you must inform your local IT Help Desk

Appendix 1

Approved Operating Systems

- iOS N-2 (where N is the latest version)
- Android N-2 or higher
- Windows N-2 or higher

Rowan Preparatory School

School iPad Agreement for Staff

- The iPad and case issued to you is the property of Rowan Preparatory School, loaned to you for the duration of your employment or until a request is made for its return.
- You are the designated user of the iPad allocated to you, identified by its serial number and the label affixed to the front of the iPad of which must not be removed.
- The iPad is connected to your school email account and therefore may have access to the personal information of pupils. This means you must fully comply with Rowan Preparatory Schools' data protection policy.
- It is your responsibility to inform Ian Jackson (IT & Facilities Manager) or a member of SLT as soon as possible if the iPad is lost or stolen.
- The iPad may be 'remotely wiped' (all content deleted) by Rowan Preparatory School if the content on the iPad is thought to be in jeopardy by the iPad being lost or stolen.
- The school will provide a standard collection of apps for use on the iPad. In addition it may provide some specific apps related to your role or department. These apps must not be deleted from the iPad at any time and any non-work related apps for personal use should not be installed.
- You should take all reasonable precautions to protect the content on the iPad and a passcode must be enabled at all times.
- Any personal content on the iPad must not breach the Rowan ICT Acceptable Use Policy.
- The school may request the return of the iPad at any time without notice for inspection purposes.
- The iPad must be enclosed in its designated case at all times.
- If you should leave the employment of Rowan Preparatory School, the iPad, case and charger must be returned to Ian Jackson (IT & Facilities Manager) before you leave.
- Photographs or video of pupils are prohibited on iPad devices that are taken off-site e.g. taken home.
- Photographs or video of pupils for the purposes of Teaching and Assessment may be allowed provided that:
    - The iPad is based permanently in school.
    - The activity complies with the school's Child Protection, e-Safety, ICT Acceptable Use and Health and Safety Policies.
    - The photos/videos are not stored on the iPad for an extended period beyond the time required for their use.
    - That the photos/videos are only backed up to the school network system.
- The school reserves the right to be make reasonable modifications or additions to this agreement and to notify signatories to that effect.
- This iPad will be checked occasionally for updates and for compliance with school policies. Outcomes will be reported to the Headmistress or Business Manager.
- Breach of this agreement may result in the school requesting the return of the allocated iPad and further disciplinary action being taken.

I have read, understood and agree to the above conditions and accept the loan of a school iPad.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the most recent e-safety policies.

Signature: ....**Date:** ....

Full Name: .... (printed)

Job title:………………………………………………...

iPad Serial:……………………………………………..

iPad Model: iPad Air 2, 16GB, White/Silver

Authorised Signature (Headmistress)

Signature: .... ………………………………………………… **Date:**..........................

Full Name: .... (printed)