United Learning Online and E-Safety Policy

Avonwood Primary School
The best in everyone™
Part of United Learning

United Learning Online Safety Policy

Date of last central office review:	August 2023	Review Period:	Annually (minimum)
Date of next central office review:	August 2025	Owner:	Group Safeguarding Lead
Date of next school level review:	September 2025		
Type of policy:	United Learning Policy	Local Governing Body	Approves Policy.

Contents

1. Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	February 2024
The implementation of this online safety policy will be monitored by the:	Charlotte Harris – Online Safety Coordinator Kim Williams – DSL
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed as necessary:	SSCT, LA Safeguarding Officer – Sue Wickins, Frazer Smith UL, LADO, Dorset Police.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering.
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

2. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of Avonwood Primary school. The 2011 Education Act increased these powers with regards 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 online safety behaviour that take place out of school.

3. Aims

Avonwood Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

4. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

5. Roles and responsibilities

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

5.1 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

A member of the senior leadership team and a governor, to be responsible for ensuring filtering and monitoring standards are met.

The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety, monitor online safety logs as provided by the designated safeguarding lead (DSL) and ensure the effectiveness of filtering and monitoring is regularly reviewed (at least annually).

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The governor who oversees online safety is Lucie Barton-Ridges and is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This will be carried out by the LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of Online Safety Governor and this role includes:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant LGB meeting

5.2 The Headteacher and Senior Leadership Team

- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and should refer to the safeguarding policy and acceptable use policy.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles. They will document decisions on what is blocked or allowed and why. The monitoring and filtering system is called Lightspeed.

- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

5.3 The designated safeguarding lead

Details of the school's DSL/DDSLs are set out in Annex C of Keeping Children Safe in Education (DfE).

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on My Concern and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Overseeing checks to filtering and monitoring systems

5.4 Network Team Manager and IT staff

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, lightspeed filtering which is updated on a regular basis and keeps pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Continuous security checks and monitoring of the school's ICT systems are made. A full assurance check is completed yearly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;

5.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use; (See Appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

5.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read (where age appropriate), understood and agreed to the terms on acceptable use of the school's ICT systems and internet (See Appendix 1).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody
- CEOP - CEOP Safety Centre
- Childline - Childline | Childline

5.7 Visitors and members of the community

Visitors and members of the community who access Avonwood school's systems or programmes or use the school's ICT systems or internet as part of the wider school provision will be made aware of this policy (when relevant) and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a Community User AUA before being provided with access to school Wi-Fi and system. (See Appendix 1)

5.8 Pupils

- are responsible for using the school's digital technology systems in accordance with the pupil's home school agreement. (See Appendix 2)
- 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 online bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

6. Education/Training

6.1 Educating 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 online safety/digital literacy is therefore an essential part of Avonwood's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

Under the new requirement, **all** schools will have to teach:

- Relationships education and health education in primary schools
- This new requirement includes aspects about online safety. As such we've added these expectations in italics below

The National Curriculum for each phase is as follows:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

The Education for a Connected World framework is as follows:

The Digital knowledge and skills that children develop through primary school includes:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

The RSE curriculum for Primary Schools is as follows:

By the **end of primary school**, pupils will know:

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.*
- *How information and data is shared and used online.*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*

The safe use of social media and the internet will also be covered in other subjects where relevant.

6.2 Educating Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children 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 of internet safety to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,

- Parents/carers evenings/sessions
- High profile events/campaigns e.g., Safer Internet Day
- Reference to the relevant web sites/publications (National Online Safety)
- Twitter: @avonwood_ICT

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6.3 Educating the wider community

The school will provide opportunities for local community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

6.4 Educating and training staff/volunteers.

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g., from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

6.4 Educating and training staff/volunteers.

Members of the LGB should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

This may be offered in several ways:

- Attendance at training provided by the Local Authority/United Learning/National Governors Association/or other relevant organisations.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

7. Protecting children from online abuse

Taken from the NSPCC "Protecting children from online abuse"(23.12.2020)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online, or the perpetrator may arrange to meet the child in person with the intention of abusing them.

7.1 Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and the anti-bullying policy)

7.2 Emotional Abuse

Emotional abuse is emotional maltreatment of a child, which has a severe and persistent negative effect on the child's emotional development (Department for Education, 20171; Department of Health, 20172; Scottish Government, 20143; Wales Safeguarding Procedures Project Board, 20194). It's also known as psychological abuse.

Most forms of abuse include an emotional element, but emotional abuse can also happen on its own.

Children can be emotionally abused by anyone:

- parents or carers
- family members
- other adults
- other children

Online examples of emotional abuse can include (but are not limited to):

- verbal humiliation
- name-calling
- criticism
- restricting social interaction
- exploiting or corrupting
- encouraging a child to take part in criminal activities.
- forcing a child to take part in activities that are not appropriate for their stage of development.
- terrorising
- threatening violence
- bullying
- deliberately frightening a child
- deliberately putting a child in a dangerous situation

7.3 Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery).

This is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it, is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

7.4 Sexual abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish Government, 2014; Wales Safeguarding Procedures Project Board, 2019). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not.
- forcing or encouraging a child to take part in sexual activity.
- making a child take their clothes off or touch someone else's genitals.
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus.

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts.

- not taking proper measures to prevent a child being exposed to sexual activities by others.
- making a child masturbate while others watch.
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images.
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

7.5 Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2018; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2019).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.

Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity
- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be

too scared to tell anyone what's happening because they don't want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online.
- send or post sexually explicit images of themselves.
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

7.6 Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-to-face by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However, extremists attempt to influence vulnerable people, the internet invariably plays some kind of role … being widely used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos and friend lists.

7.7 The school's response to online abuse

To help prevent online abuse we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss examples of online abuse with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on examples of online abuse to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online abuse, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

8. Mobile Technologies (including BYOD)

For more information, please refer to the school's BYOD policy: (See Appendix 3)

Please also refer to the school's Mobile Device and Phone policy.

9. Use of digital and video images

Please refer to United Learning Copyright Policy:
https://hub.unitedlearning.org.uk/sites/policies/technology/pages/default.aspx?groupid=12#item21

10. Data Protection

When sharing information staff will ensure they comply with group data protection policies and keep records of disclosures as required by these policies.

11. Technical – infrastructure/equipment, filtering and monitoring

The United Learning Trust will be responsible for ensuring that the Avonwood's network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Avonwood's technical systems will be managed in ways that ensure that the school meets recommended technical requirements as set out in the Department for Education's "Meeting digital and technology standards in schools and colleges"
- There will be regular reviews and audits of the safety and security of Avonwood's technical systems.

- There will be regular reviews* (at least annually or when: a safeguarding risk is identified, there is a change in working practice and/or new technology is introduced) and checks** of the safety and security of the school's technical systems. These will be recorded.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Avonwood's technical systems and devices.
- All users at Key Stage 2 and above will be provided with a username and secure password by Salamander software who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- United Learning/Avonbourne's IT Team 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Filtering requests are made via the school's helpdesk, where deemed appropriate which are then raised with the safeguarding lead and the head teacher.
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.** N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- The school has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users – staff and pupils.
- Avonwood's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breaches to the GDPR lead.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users' staff/pupils and community users and their family members are allowed on school devices that may be used out of school. (See Appendix 1)
- An agreed policy is in place (acceptable use policy) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See Appendix 1)

12. How the school will respond to issues of misuse

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Specific pupil/staff misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

*Any review will need to understand:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

** Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

13. References, further reading and useful links

GOV.UK (30.6.2020), 'Guidance: Education for a Connected World', Available at: https://www.gov.uk/government/publications/education-for-a-connected-world

LGfL (2021), 'Online Safety and Safeguarding', Available at: https://www.lgfl.net/online-safety/default.aspx

National Online Safety (2021), 'Online Safety Education for the Whole School Community', Available at: https://nationalonlinesafety.com/

NSPCC Learning 23.12.2020), 'Protecting children from online abuse', Available at: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

SWGfL (2020), '{school/academy} Online Safety Policy Template', Available at: https://swgfl.org.uk/assets/documents/online-safety-policy-templates-without-appendicies.pdf

The Key (23.12.2020), 'Online safety policy: models and examples', Available at: https://schoolleaders.thekeysupport.com/policy-expert/pastoral/online-safety-policy-model-examples/#section-0

United Learning (2021), 'Policies Portal', Available at: https://hub.unitedlearning.org.uk/sites/policies

Appendix 1 - United Learning ICT Acceptable Use Policy

Adopted by the Finance & Infrastructure Committee, July 2015

All employees must read and sign this Acceptable Use Policy before they can be allowed to use devices or services provided by or on behalf of United Learning. In signing this policy, you agree to the following:

a. An authorized representative of the Group may view, with just reason and without notice or notification, any communications you send or receive, material you store on the Group's computers/ services or logs of websites you have visited. This data, regardless of where hosted, belongs to United Learning at all times. It is the Group's policy not to view colleagues' emails without good cause.
b. You will only access those services/ aspects of services which you have been given permission to use.
c. You will not use United Learning resources to operate your own business.
d. You will not attempt to remove any of the security measures put in place by United Learning to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.
e. Any communication from a United Learning related account (email, social media) or account which identifies you as belonging to United Learning will be appropriate in tone and content.
f. You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of Data Protection legislation.
g. You will not transfer United Learning data outside of the organisation's systems except via Group email or encrypted media. This includes the use of cloud storage and personal email accounts. *For example, saving files to Dropbox or emailing them to a personal Hotmail account may resolve logistical problems you are having but run the risk of those data leaving United Learning's control.*
h. You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include gambling (outside of workplace Lottery syndicates), pornography and sites promoting views which run counter to the organisation's ethos.
i. You will not share your access credentials with anyone. Delegated access to calendars/ email should be granted to administrative support staff, where required.
j. You will not download, use, distribute or otherwise communicate any material which, in so doing, infringes copyright.

k. The use of language deemed aggressive, offensive or intimidating is not acceptable. You must not write anything on a website or send anything by email or another medium, anything which could be reasonably be deemed offensive.

l. Use of a personal device to access any United Learning data is permitted, subject to the acceptance of the separate Bring Your Own Device policy.

m. Breach of this policy may result in disciplinary action.

Name:	
Signature:	
Job Title:	
Date:	

Please return your completed form to the HR team.

Appendix 2 – Home School Agreement

AVONWOOD PRIMARY SCHOOL

HOME/SCHOOL AGREEMENT

Name of child:

……

At Avonwood Primary School, we recognise each child as an individual, and aim to give all children every opportunity to realise their full potential. We believe that a close partnership between the school, parents and the child is essential if we are to achieve this aim. We therefore ask all parents and children to sign up to our Home/School Agreement.

The Responsibilities of the School

At Avonwood Primary we will:

- Provide a secure, happy and stimulating learning environment.
- Provide a broad and balanced curriculum which challenges your child to reach their potential and fulfils the requirements of the National Curriculum.
- Encourage your child to show friendship and respect for others and to abide by the school behaviour policy, ensuring a safe, caring environment for all.
- Keep you informed about your child's progress and behaviour, as well as their termly curriculum.
- Set regular and appropriate home learning for your child.
- Make you feel welcome whenever you visit the school and respond to your questions or concerns as quickly as possible.
- Always treat parents in a respectful and polite manner.
- Allow children safe and secure use of the Internet through a combination of site filtering, supervision and by fostering a responsible attitude in all pupils, in partnership with parents.
- Respond to any concerns in a timely and professional manner.

Signed:

(On behalf of Avonwood Primary School)

The Responsibilities of the Parents/Carers

All parents/carers will:

- Having chosen Avonwood Primary School for your child, accept the school's aims and values, positively supporting the school.
- Ensure that your child attends school punctually every day during term time, unless there is a good reason for absence (e.g., illness).
- Notify the school by letter or telephone in the event of absence.
- Respect our policy of no term time holidays (see the website for further details)
- Uphold our expectation for Avonwood to be a 'Smart Phone' free site for children.
- Transport their child to and from school in a safe manner.
- Make sure an appropriate known adult always drops their child to class (to the door) and collects on time, in Years EYFS through to Year 6.
- Support the school's policies and guidelines on learning, behaviour and uniform, both in School and at home.
- Attend parent/teacher consultations to discuss your child's progress.
- Keep us informed of where to contact you in case of emergency.
- Promptly inform the school of any concerns or problems that may affect your child's learning, behaviour or happiness at school.
- Follow and uphold our uniform policy including expectations around jewellery, hairstyles and clothing.
- Support school in the teaching of safe and secure Internet use at home.
- Contact the school prior to raising concerns or complaints on social media (e.g., Facebook / WhatsApp)
- Use the car park when required but only ever parking in appropriate spaces. If parking offsite, parents will be respectful of our neighbours and any parking restrictions.
- Please read our school policies, which can be found on our website.
- Support your child with home learning, including daily reading together.
- Reach out to staff for help and support when required.
- Be polite and respectful to all members of the school community.

Signed: …… (Parent/Carer) Date ……

The Responsibility of the Child

I will try my best to:

- Do all class learning and home learning as well as I can, asking questions when I don't understand.
- Be respectful towards others and behave in a safe and responsible way.
- Be kind, helpful and forgiving.

- Be honest.
- Try my best to be on time daily, always walking side by side with my adults to and from school.
- Wear a helmet if I ride a bicycle or scooter.
- Wear appropriate uniform to school, such as a cap in the summer.
- Never bring a Smart Phone to school without written consent from the Headteacher.
- Behave appropriately if I attend any after school clubs.
- Use the Internet safely as I have been taught in class.

Signed: …… (Child) Date ……

Appendix 3

Bring Your Own Device (BYOD) Policy - accessing United Learning data

1. Introduction

1.1. Under the GPDR and the Data Protection Act (DPA) 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 and at home; "personal devices" includes but is not necessarily limited to mobile phones (both standard and smart), 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. Google G-Suite is free of charge for education and can also be used where applicable.

Office 365 enables remote workers to use the software within a browser eliminating the need for a local installation or any local copies of data.

3. General principles for keeping data secure.

3.1. Data must always remain within United Learning systems – **emails must not be forwarded to private accounts** and files should only be stored within OneDrive/Google Drive rather than saved locally (to the desktop or C drive for example).

3.2. Data containing Personally Identifiable Information (PII) must not be used in a locally installed program in the Office 365 suite. PII must only be used in the browser-based versions of the software.

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

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

3.5. 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/Apple Macs is allowed if separate accounts are set up, the account being used for work is completely separate, account details are not shared, and passwords meet the required United Learning complexity levels. Other accounts on the device must not be 'Admin' type accounts that grant access to other areas of the device.

3.6. 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.

3.7. 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: -

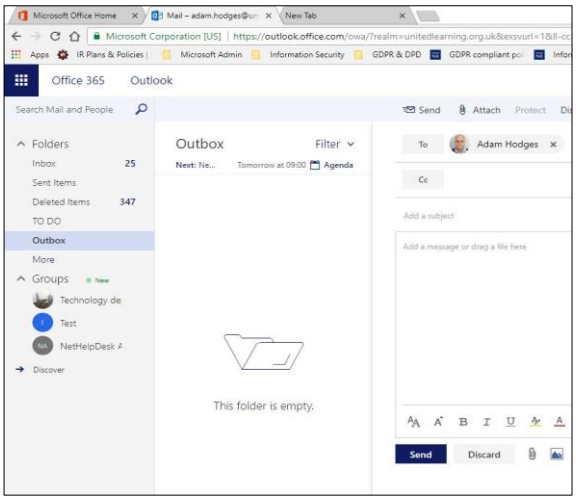
Section A (Browser)

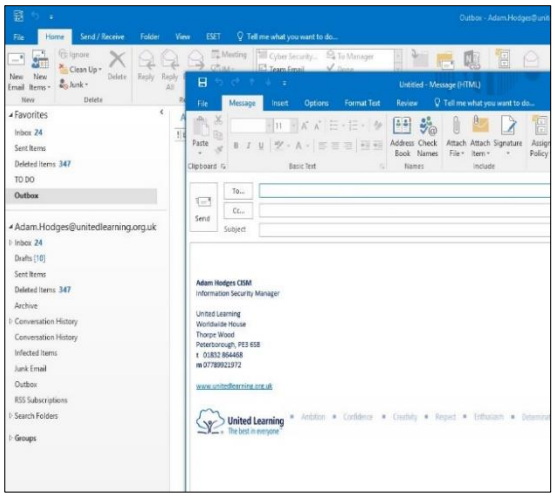
I want to download United Learning or school data to my device and work on these with the native/ desktop applications e.g., Mail for iPhone, Office 2016, Outlook.
Go to: -

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.





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

SECTION A

Accessing data and systems through a browser

1.1. You will only access Microsoft O365 (Word, PowerPoint, Outlook, OneDrive, SharePoint etc) or G-Suite applications from within a current browser. Office 365 and G-Suite are designed to work with the current versions of Chrome, Edge, Firefox, and Safari. Internet Explorer, while it will still work will not be supported beyond Summer 2021 – and MS Teams support will end in November 2020.

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 (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 all 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. If 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 (or G-Suite) 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

Using your own device

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?**

    1.1. Your device must use one of the Operating Systems and versions listed in Appendix 1

    1.2. 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.

    1.3. You must agree to install a satisfactory anti-virus program on the device used for BYOD under this policy.

    1.4. 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.

    1.5. You must agree to protect your device via a complex password (8 characters or greater, including three of the following - numbers, upper-case, lower-case letters and special characters) or a biometric measure. Please see here for the United Learning Password Policy.

    1.6. 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.

    1.7. 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.

1.8. You must keep any personal data separate from United Learning data. The simplest way to achieve this is to use the G Drive/OneDrive client (NB not the OneDrive Sync client) which your IT Help Desk will set up for you.

1.9. 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.

1.10. 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.

1.11. 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.

1.12. 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.

1.13. 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.

1.14. 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.

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

2. 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 for your United Learning Academy 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 to be 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 an appropriate Anti-Virus product installed?	Choose an item.	☐
	If so, which Anti-Virus product 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?	Choose an item.	☐
7.	Does the applicant have the only Admin account	Choose an item.	☐
8.	Is the device encrypted?	Choose an item.	☐
9.	Has the process for reporting a lost device been explained?	Choose an item.	☐
10.	Has the level of support been explained?	Choose an item.	☐
11.	Has the register of devices been updated?	Enter Device Name.	☐

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

Signed by Technician: Click or tap here to

3. 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: As at August 2020 the "Best iPhone AV product" is, as judged by end users, Avast Security & Privacy

Android devices: We recommend Sophos from the Play Store - 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 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

macOSX: follow the advice here - https://support.apple.com/en-gb/HT202860

Apple Devices (iPhone, iPad, or iPod touch)**:** - 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

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

macOSX: 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 into 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