Online Safety Policy

The Chantry School

September 2021

Responsible:	AD	
Approved by:	FGB	**Date: 9th December 2021**
Last reviewed on:	November 2021	
Next review due by:	September 2022	

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/committee made up of:

- Headteacher and senior leaders
- Online Safety Coordinator
- Staff – including teachers, support staff, technical staff

The following will be invited to contribute to future revisions through the Online Safety Group

- Governors
- Parents and carers

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 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 the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. Further information is provided in Section 15 of the January 2018 DfE Searching, Screening and confiscation Document for Schools.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf)

In the case of these 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.

Related Documents

- The Chantry School Safeguarding Policy
- The Chantry School GDPR Policy
- The Chantry School Online (Remote) Learning Policy
- The Chantry School Behaviour Policy
- The Chantry School Anti-Bullying Policy

1. Key responsibilities of the community **AD**

1.1 Key responsibilities of Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports through the regular safeguarding reports. A member of the Governing Body has taken on the role of Online Safety Governor – this is the same governor who is designated as Safeguarding Governor. The role of the Online Safety Governor will include:

- 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 Governors

1.2 Key responsibilities of Senior Leadership Group

- 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 (at least) 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. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant disciplinary procedures).
- 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 also support to those colleagues who take on important monitoring roles. This will be in the form of regular meetings with their line manager.
  The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead

1.3 Key responsibilities of the designated safeguarding/online safety lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority or other relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends / reports to relevant meetings of Governors.
- reports regularly to Senior Leadership Team

1.4 Key responsibilities of all staff

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy (AUP)
- they report any suspected misuse or problem to the Headteacher or other Senior Leader or Online Safety Lead or Head of Year for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/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

1.5. Key responsibilities for staff managing the technical environment

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any relevant body online safety policy/guidance that may apply.
- 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 (*see* appendix "Technical Security Policy Template" for good practice*)*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead or Heads of Year for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school/academy policies

1.6 Key responsibilities of students are

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- 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/academy's* online safety policy covers their actions out of school, if related to their membership of the school

1.7. Key responsibilities of 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, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school/academy (where this is allowed)

1.8 Key responsibilities of Online Safety Group

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

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead (or other relevant person, as above) with:

- the production/review/monitoring of the school online safety policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified e.g. through use of the 360 degree safe self-review tool

2. Online Communication and Safer Use of Technology **JB / DD / JD**

- Login details for the website are controlled by the network manager and only given to users who have been trained on the website.
- Any images or videos that are uploaded to the internet must be checked and approved. Any pupils need to have consent for their image to be published. If this is not given but the video needs to be uploaded the video needs to be sent to ITsupport@chantryschool.com so the pupils face can be blurred out.
- Emails are assigned when pupils/staff start and are removed at the end of their official leaving date. Access can be extended with approval of the LMT.
- Webcams and visualisers are in every classroom. These are to be used for remote learning and approved calls to outside organisations only. Backgrounds should be blurred and pupils only shown if for an approved use e.g calling another school to do a talk between classes.
- All internet connections in the school are filtered through RM safetynet. Staff and Pupils have different levels of filtering except when using the BYOD which will use the strictest level of filtering possible. All use of school computers in monitored via Impero. Impero has built in safeguarding and PREVENT word lists which get flagged. Checked by IT everyday for any serious breaches. This software takes screenshots so context of the alert is available.
- Pupils and staff have access to school data remotely. This is through Office365 protected by multifactor authentication or through the remote server. To download the remote server file a user has to login to Office365.

3 The Chantry School Social Media Policy **(AD)**

This policy is based on the NEU model policy, and has been updated in our Code of Conduct for school use from September 2020.

The Chantry School recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Purpose of the policy

- The purpose of this policy is to encourage good practice, to protect the school and its employees, and to promote the effective use of social media as part of the school activities.
- This policy covers personal and professional use of social media and aims to encourage its safe use by the school and its employees.
- The policy applies regardless of whether the social media is accessed using the school's IT facilities and equipment, or equipment belonging to members of staff.
- Personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's reputation are within the scope of this policy.
- This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.

Roles, responsibilities and procedure

Employees should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer;
- be aware that any excessive use of social media in school/college may result in disciplinary action;
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the trust, or even future employers, to read. If in doubt, don't post it!
- ensure they protect themselves both in what they post, and how they set up their social media accounts.
- Not use social media for routine work communications. Departments and colleagues may have created their own social groups, but routine and regular work communications should take place through school systems e.g. Teams / email.

The headteacher or his nominated representative is responsible for:

- addressing any concerns and/or questions employees may have on the use of social media;
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.
- implementing and reviewing this policy.

Human resources (HR) is responsible for:

- giving specialist advice on the use of social media;

Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace, Flickr and YouTube. This list is not exhaustive, but intended to be representative.

Acceptable use

Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

Employees should not upload any content on to social media sites that:

- is confidential to the school/trust or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school/trust into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the school/trust's social media accounts. Employees should note that the use of social media accounts during lesson time is not permitted.

Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- online bullying;
- grooming, exploitation or stalking;
- exposure to inappropriate material or hateful language;
- encouraging violent behaviour, self-harm or risk taking.

In order to mitigate these risks, there are steps you can take to promote safety on line:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos or information comply with existing policies.

Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the school/trust.
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Reporting, responding and recording cyberbullying incidents

- Staff should never engage with cyberbullying incidents. If in the course of your employment with this school/trust, you discover a website containing inaccurate, inappropriate or inflammatory written material

relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager at your school.
- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

Action by employer: inappropriate use of social media

- Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation.
- If in the course of the investigation, it is found that a pupil submitted the material to a website or social media platfrom, that pupil will be disciplined in line with the school's behaviour policy.
- The senior manager, where appropriate, will approach the website hosts or social media platform to ensure the material is either amended or removed as a matter of urgency. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.
- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will make every endeavour to contact the internet service provider (ISP) (as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website).
- If the material is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police or support the member of staff in their own reporting.
- The member of staff will be offered full support by the employer at all stages of the action.

Breaches of this policy

Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the school/trust's bullying or disciplinary procedure. The member of staff will be expected to co-operate with the school's investigation which may involve:

- handing over relevant passwords and login details;
- printing a copy or obtaining a screenshot of the alleged unacceptable content;
- determining that the responsibility or source of the content was in fact the member of staff.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school/trust or the individuals concerned. Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee. Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

Monitoring and review

If the manager reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the school/trust's network.

This policy will be reviewed on an annual basis (as part of the Code of Conduct) and, in accordance with the following, as necessary:

- legislative changes;
- good practice guidance;

- case law;
- significant incidents reported.

This policy does not form part of any employee's contract of employment and may also, after consultation with the trade unions, be amended from time to time by the school/trust.

Legislation

Acceptable use of social networking must comply with UK law. In applying this policy, the school/trust will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

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. When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment. Staff should use discretion and common sense when engaging in online communication.

4 Use of Personal Devices and Mobile Phones

4.1 Student BYOD protocols **MP**

The Chantry School recognises that student devices can be a useful tool for learning. Students are allowed to use mobile devices in the classroom to assist them in their learning activities only when the teacher has given explicit permission using the traffic light system, and when parental permission has been granted. An up-to-date list of pupils without parental permission can be found in the staff shared area.

All staff will display the BYOD (Bring Your Own Device) traffic light control system poster in their classrooms and make clear reference to whether the lesson is red/amber/green. See appendix for version.

Use of 4g on devices is not permitted. Pupils will only use the Chantry BYOD password to connect to the internet. The password is Chantry-1963. Where pupils are given the "green light" to use their own devices, teachers will explicitly remind all pupils that devices are to be connected in this way.

Students can listen to sound only if instructed to by the teacher. Pupils must use their own headphones. No music is to be played aloud unless with instruction from teacher.

The use of devices may vary according to subject areas, but some possible uses are:

- Completing assignments or quizzes on Microsoft Teams
- Quiz style platforms such as Quizlet, Kahoot, Blooket
- Memrise and Language Gym
- Accessing BBC bitesize to complete research or quizzes
- Dictionary/thesaurus
- Calculator
- Research
- Other subject related apps

Staff will not ask pupils to photograph or video other pupils using their own devices.

We expect that students will all use their devices sensibly and in a manner which supports learning. However, there will be clear consequences for misuse of devices.

	Description of misuse:	Action taken:
Step 1:	Initial misuse (eg. Using device without permission or for unrelated lesson content)	Verbal warning
Step 2:	Continuing to misuse device (eg. Continuing to use device without permission or for unrelated lesson content)	C3 detention
Step 3:	Severe misuse (eg. Completely disobeying rules for devices or continuing to misuse device)	C4 detention and confiscation of device

This is not an exhaustive list, but types of misuse may include:

- Using the device without teacher permission
- Connecting the device to a personal mobile network (via the SIM card) and accessing unfiltered websites (e.g., YouTube, Facebook)
- Listening to music on a device when it is not linked to the teaching & learning which is taking place
- Devices producing sound without permission
- Using the device for non-work-related activities

Gross misuse might include:

- Deliberately viewing inappropriate websites
- Filming or photographing other students or teachers
- Having inappropriate material or images stored on the device

4.2 Student mobile phone policy **ML**

- Pupils are allowed to bring to school at their own risk a mobile phone / device to be used in the classroom for the purpose of BYOD learning activities.
- The school is not responsible for the loss / theft or any damage to the device.
- Pupils may use their device on school transport responsibly – with headphones as not to disturb anyone else including the driver on the bus.
- Pupils should not access anything on their device that is unlawful, lewd, may cause harm, distress or offence to anyone else on their bus, either intentionally or unintentionally.
- Pupils must have their device switched off once arrived on school grounds – either the Yard or car park.
- Pupils may not switch their device on until they have been dismissed from Period 5 and have left the school buildings. The exception to this rule is by direction from a teacher for the purpose of a BYOD activity.

4.3 Staff use of own devices (See also Working in The Chantry School Code of Conduct)

- Personal mobile phones brought into school must have a passcode.
- Staff may use their personal mobile phone on the school site, provided they are not doing so within sight of pupils and for short periods of time to make essential calls and arrangements. In general, this means in the staff room, offices and classrooms when pupils are not present. Clearly, however, staff are at a place of work and the school expect your time to be used productively to that effect.

- Staff are advised to ensure that facilities such as Airdrop are set to ensure only known contacts are able to share images with you.
- Staff must not photograph pupils using their own photographic equipment or mobile phone.
- Staff must only communicate with pupils using official school equipment or email addresses. They must not use their own device to communicate. The exception to this may be in an emergency / critical incident when their own number must be hidden.

5. E Safety Education and Engagement **JD**

5.1 Engaging Students

At the Chantry School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum. Therefore, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

In addition to this, within the KS3 computing curriculum, we deliver a Digital Lives curriculum to raise awareness about the broad impact on students of their digital use. Students learn:

- What constitutes safe use of online and digital technologies.
- The importance of showing kindness and respect to others when using technology.
- How to understand their online identities and what this means for their offline world.
- The problems that can occur as a result of the over-use of digital technologies and how to manage their online time.
- The laws related to digital use.
- What a digital footprint is and the problems these can cause as they grow older.
- How to recognise the risk of fake news and how to be more critical in their reading of online materials.
- How to adopt healthy emotional well-being habits in a digital world.

Within KS4, the students that select Computer Science for GCSE study an in-depth unit looking at cyber security as well as learning about the morals and ethics of computer technology. These enhance their existing knowledge of e-safety and associated issues learned at KS3.

We will also provide students with other opportunities in school to understand best practices in digital use by:

- Making the student Acceptable Use Policy easy to access on the school network.
- Rewarding positive use of technology with reward points.
- Recruiting Digital Assistants in lessons to promote responsible use of technology and peer education in problem solving issues.
- Recruiting Digital Leaders from every year group to promote safe, effective and positive use of technology.
- Running assemblies with the Digital Leaders to focus on areas of e-safety.
- Providing PSHE lessons and tutorial sessions focusing on e-safety.
- Running student voice and surveys about e-safety and technology use.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Engaging Parents / Carers

The Chantry School recognises that parents/carers have an essential role to play in enabling students to become safe and responsible users of the internet and digital technology.

Parents'/carers' attention will be drawn to the Chantry School's e-safety policy and expectations in communications, such as letters and the school's website.

We will build a partnership approach to e-safety with parents/carers by:

- Providing information and guidance on online safety in a variety of formats.
- This will include making useful website resources available on the school website and keeping these updated (www.chantryschool.com/safeguarding/), posting relevant information on the school's social media platforms, offering specific e-safety awareness training and highlighting e-safety at other events such as parent evenings, transition events and curriculum evenings.
- Requesting that they read e-safety information as part of joining our community, for example, within our home-school agreement.
- Requiring them to read our student acceptable use policy and discuss the implications with their children.

5.3 Responding to concerns **ML**

- Any concerns should be reported on CPOMS immediately
- Any concerns with a child-on-child or adult-on-child sexual concern including the sharing of nudes and semi-nudes should be reported to the DSL / DDSL immediately.
- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent)
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.

6 Managing Information Systems **JB / DD**

6.1 Managing Personal Data

We aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

There is a Data Protection Team in school who manage procedures around data protection. The Data Protection Policy explains the principles of data sharing with definitions. It identifies roles and responsibilities and processes for handling data requests. It includes how we deal with biometrics, photographs and video. The policy also considers how we deal with a data breach and how we store and dispose of data.

Please refer to the Data Protection Policy 2021 for more details.

6.2 Security and Management of Information Systems

The school will be responsible for ensuring that their infrastructure/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 receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school/academy meets recommended technical requirements.
- there will be regular reviews and audits of the safety and security of school/academy 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/academy systems and data.
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- all users will have clearly defined access rights to school. Access is assigned through principle of least privilege.
- 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 Network 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* following the school BYOD policy.
- Technical staff regularly monitor and record the activity of users on the school/academy technical systems and users are made aware of this in the acceptable use agreement. Internet access is monitored using RM Safety Net. Computer use is monitored using Impero.
- Impero is used by staff to control workstations and view users activity.
- The IT helpdesk ITsupport@chantryschool.com is used to report any technical incident to the technical team.
- an agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system. Supply teachers each have access to a "supply" account to be used. Each is given to only one teacher and recorded. Trainee teachers have a full staff account created when authorised by the coordinator which is disabled when they leave.
- Executable files cannot be downloaded by users. Any software must be preapproved by the Network Manager.
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school/academy devices. Staff must have any removable media encrypted before it is allowed on the school network. Pupils are not allowed to use removeable media.
- the school/academy 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/academy site unless safely encrypted or otherwise secured.

6.3 Password Policy

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school/academy technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

Policy Statements:

- These statements apply to all users.
- All school/academy networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school/academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and students/pupils) 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.
- Passwords must not be shared with anyone including the technical staff.
- All users will be provided with a username and password by the technical staff who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/academy. Your network password must never be used in any external systems.
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system
- *Google Chrome can be used to generate complex passwords to websites that are stored in your Google account using your school email address.*
- *Passwords are not set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

Learner passwords:

- Users will be required to change their password if it is compromised or if multiple suspected compromised accounts as a precaution.
- Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- An administrator account password for the school/academy systems should also be kept in a secure place e.g. school/academy safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by* the technical team for staff. *All members of staff can reset a pupil password which must be changed at first login.*
- *Requests for password changes should be authenticated to ensure that the new password can only be passed to the genuine user. Pupils need to be in school to get a new password or only sent to contacts listed in the MIS. Staff passwords can only be given out face to face or to a secondary email address listed in the MIS. Passwords must never be given out over the phone.*
- Accounts are locked for 10 minutes if the incorrect password is entered 3 times. Pupils can ask staff to unlock their accounts. Staff must see the technical team to have their account unlocked

6.4 Resilience

- Resliience of data and access must be maintained as a priority.
- The school runs a fail over cluster configuration to allow one physical host to be powered down or in a fault state and all the virtual servers will fail over to the remaining host.
- Storage is on a SAN in 2 virtual disks both configured in RAID5 to allow one disk fault tollerance.
- Backups of the data are essential in the event of lost data, rollbacks or disaster recovery.
- Daily backups are made every weekday and kept for 3 weeks.
- Weekly backups are made every Satuday and kept for 4 months.
- A Termly backup is made at the end of every school term and kept for 2 years.
- Offline backups are made 3 times a week and are only online during the backup window. These are rotated so ensure in the event of ransomware while one is running we can restore to the previous offline backup.

7. Appendices

7.1 Student Acceptable Use Policy **(JD / LW)**

The school has provided computers for use by students, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support learning.

The computers and IT equipment are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible

for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Safe

- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences.
- I know that my use of school computers, devices and internet access will be monitored and filtered to protect me and ensure I comply with the school's acceptable use policy.
- I am aware that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts.

Private

- I will keep my passwords private. (If I think someone has learnt my password I will change it immediately.)
- I will never use someone else's logon name or password to access any school systems.
- I will always ensure I have completely logged off a PC before leaving it.
- I will think before I share personal information and/or seek advice from an adult.
- I will not share other people's personal data without their permission.

Responsibility for school equipment

- I will not attempt to install any software or hardware on the school computers.
- I will NOT use external storage devices such as USB sticks on the school network.
- I will only change the settings on a computer if a teacher/technician has allowed me to.
- I will not eat or drink in any of the IT rooms.
- I will not use a staff member's computer including the attached audio/ visual equipment unless I have explicit permission to do so.
- I will not misuse my printing privileges and will only print school related work documents.

Responsibility for internet access

- I will only use the internet for educational purposes.
- I will only download materials or images which are relevant to my studies.
- I will always check that any information I use online is reliable and accurate.
- I will not copy information from the internet into my work without acknowledging the source (plagiarism).
- I will never disclose or publicise personal information online.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.

Responsibility for email / Teams messaging

- I will use my school email and Teams accounts for educational use only.
- I understand that the use of strong language, swearing or aggressive behaviour and sending of inappropriate content is not tolerated.
- I understand that I should only open attachments on emails if they come from someone I already know and trust and understand that attachments can contain viruses or other programs that could destroy all the files and software on my computer and the school network.
- I understand that if I receive an email or message containing material of a violent, dangerous, racist, or inappropriate content I will always report such messages to a member of staff.
- I understand that bulk emailing or spamming is not permitted, I will ask a member of staff if emails to groups of students or staff is required.

Kind

- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete.
- I will not use technology to be unkind to people.

Legal

- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.

Report

- If I am aware of anyone trying to misuse technology then I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable.
- I will visit useful websites (www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk) to find out more about keeping safe online.
- If IT equipment has been damaged or is faulty I will report this to the IT team.

Sanctions

If I do not follow the AUP then:

- I understand that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used.
- I understand access to school IT systems, including email and Teams, may be withdrawn.
- I understand the school may issue further sanctions in line with the school behaviour policy.

7.2 Staff Acceptable Use Policy **(DD / JB)**

Using the school computers and network are subject to an acceptable use policy (AUP)

- I know that my use of school computers, devices and internet access will be monitored and filtered to protect me and ensure I comply with the school's acceptable use policy.
- I will keep my passwords private.
- I will never use someone else's logon name or password to access any school systems.
- I will always ensure I have logged off or locked any computer I have been using.
- I will think before I share any data with external sources and check with ITsupport/DPO if unsure.
- I will not attempt to install any software or hardware on the school computers. Any software or hardware purchases should be checked with IT before purchase. Failure to do so can cause compatibility with the school network to not be possible.
- Any external storage device must be encrypted before use on the school network
- I will not misuse my printing privileges and will only print school related work documents.

- I will only use the internet for educational purposes. As a member of staff my internet use is subject to filtering and monitoring.
- I will only download materials or images which are suitable for the school network and within copyright/fair use.
- I will always check that any information I use online is reliable and accurate.
- I will not use any software to download videos from Youtube.
- I understand that the school's internet filter is there to protect me and the school, and I will not try to bypass it.
- I know it can be a criminal offence to hack accounts or systems.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.
- If I am aware of anyone staff or pupil, trying to misuse technology then I will report it to ITSupport to investigate.
- If IT equipment has been damaged or is faulty I will report this to ITsupport@chantryschool.com. No matter how minor as it may indicate a bigger issue.

Sanctions

If I do not follow the AUP then:

- I understand that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used.
- I understand the school misusing the IT network can be a breach of the computer misuse act and lead to disciplinary action.

7.3 BYOD Classroom Poster **(MP)**