ONLINE SAFETY POLICY & PROCEDURES

DOCUMENT CONTROL

Author/Contact	Tracey Shackley Tel: 01946 820356 Email: contactus@changinglives.education
Document Path & Filename	Staff General/Corporate Information/Policies and Procedures/Online Safety Policy and Procedures
Document Reference	Online Safety Policy and Procedures
Version	6 MAT
Status	Approved
Related Policies	See policy section page 2
Publication Date	October 2023
Review Date	Annually
Approved/Ratified by	CLLT Trust Board	
Distribution: Changing Lives Learning Trust Staff Please note that the version of this document contained within the Policy Folder on Staff General is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.		

Version	Date	Comments	Author
01	September 2010		Karen Forsyth
02	April 2011		Karen Forsyth
03	March 2012		Karen Forsyth
04	June 2013		Karen Forsyth
05	September 2013		Karen Forsyth
06	September 2014		Stephen Gilby
07	March 2016		Stephen Lester
08	October 2016	Addition to acceptable use contract	Stephen Lester
09	November 2017	Updated social media	Stephen Lester
01 MAT	May 2018	Compliance with GDPR	Stephen Lester
02 MAT	September 2018	Updated	Stephen Lester
03 MAT	September 2019		Stephen Lester
04 MAT	December 2019		Stephen Lester
05 MAT	September 2021	Updated to comply with KCSIE 2021	Caroline Stevenson
06 MAT	October 2023	Updated in line with statutory DfE guidance 'Keeping Children Safe in Education' Sept 2022.	Tracey Shackley

| | | Changed BYOD into section 9.2 to make it easier to find and reference (no content changes). Significant chunks of the Remote Learning section removed and replaced with links to government guides. Appendices removed and replaced with links to separate documents that are easier to use, update and distribute. Other links all checked as correct.
Updated in line with KCSiE 2023 (filtering and monitoring) and to various links | |

CONTENTS

Appendix A	-	**Secondary School Pupil Acceptable Use Agreement**
Appendix B	-	**Staff/Volunteer Acceptable Use Agreement**
Appendix C	-	**Member/Trustee/Governor Acceptable Use Agreement**

Online Safety – links to various useful websites
360º safe - Online safety self-review tool for schools
Sample UKSIC EYFS, Primary and Special School Online Safety Posters (**ages 3-6) (ages 7-11)**
Sample UKSIC Secondary School Online Safety Poster **(11 years and over)**
KAHSC Online Safety - Managing Filtering and Monitoring
KAHSC Model EYFS, Primary & Special School pupil/parent Acceptable Use Agreement
KAHSC Model Secondary School pupil/parent Acceptable Use Agreement
KAHSC Model Staff/Volunteer Acceptable Use Agreement
KAHSC Model Governor Acceptable Use Agreement
KAHSC Response to an online safety incident or concern flowchart

POLICY

1. BACKGROUND/RATIONALE

New technologies have become integral to the lives of children and young people in society, both in school and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access.

The requirement to ensure that children and young people can use online and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. The Trust's Online Safety Policy and procedures will help to ensure safe and appropriate use, and the development and implementation will involve all stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents, carers, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk in and outside of school. Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The risk of being targeted by extremists in order to promote and encourage radicalisation;
- The risk of being targeted by those involved in child sexual exploitation;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Being drawn into taking part in unsuitable online challenges and/or hoaxes;
- Inappropriate communication/contact with others, including strangers;
- Cyberbullying (including prejudiced based and discriminatory bullying
- Access to gambling/gaming sites:
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy, and relevance of information on the Internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other academy policies and procedures including the Overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour.

As with all other risks, it is impossible to eliminate online risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which

they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This trust must demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their families) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use.

2. DEFINITIONS

For the purposes of this document a child, young person, pupil, or student is referred to as a 'child' or a 'student' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g., carers, legal guardians etc.

Wherever the term 'Principal' is used this also refers to any manager with the equivalent responsibility for children.

3. ASSOCIATED TRUST/LOCAL ACADEMY POLICIES AND PROCEDURES

This policy should be read in conjunction with the following trust/local academy policies and procedures and, where they exist, addendums to those policies and procedures:

• Overarching Safeguarding Statement
• Child Protection Policy and procedures
• Data Protection Policy including procedures for CCTV
• Health and Safety Policy and procedures
• Whole School Behaviour Policy
• Procedures for Using Students' Images
• Whistleblowing procedures
• Code of Conduct for staff and other adults
• Voluntary Home-School Agreement

4. COMMUNICATION/MONITORING/REVIEW OF THIS POLICY AND PROCEDURES

This policy and procedures will be communicated to staff, students, and the wider community by:

• Posting it on the trust and academy websites and shared staff drives
• Making a paper copy available on request from the academy offices
• Discussing trust and local academy policy and procedures during induction with new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
• Discussing Acceptable Use Agreements with students at the start of each year
• Issuing Acceptable Use Agreements to external users of school systems (e.g., Governors) usually on entry to the trust
• Holding Acceptable Use Agreements for students, staff and governors/trustees.

The Online Safety Policy is also referenced in other trust and local academy policies and procedures as outlined above.

The review period for this policy and procedures is determined by the Trust Board and indicated on the front cover.

5. SCOPE OF THE POLICY

This policy and procedures applies to all members of the trust community (including staff, students, volunteers, parents, visitors, trustees, governors, community users) who have access to and are users of our ICT systems, both in and outside of the trust.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This includes incidents of cyberbullying (including prejudiced based and discrimatory bullying), or other online safety related incidents covered by this policy and procedures, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers in relation to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken in relation to issues covered by the published Whole School Behaviour Policy and procedures.

The trust will deal with such incidents within this policy and procedures and the Whole School Behaviour Policy which includes anti-bullying procedures and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place outside of the trust.

PROCEDURES

1. ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for online safety of individuals and groups within the trust.

1.1 Governors

The role of the governors/online safety governor is to:

- ensure a member of the governing board is elected to the role of Online Safety Governor who should then lead on relevant governance requirements below;

- ensure an appropriate senior member of staff from the leadership team is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety and an understanding of the filtering and monitoring systems and processes in place) with the appropriate status, authority, time, funding, training, resources, and support;

- ensure other roles and responsibilities are appropriately allocated to staff and third parties, e.g. external service providers in order to meet the DfE Digital and technology standards;

- ensure that systems are in place to meet the requirements of the DfE Cyber security standards. Schools must have a Cyber security and resilience strategy in place which is supported by an appropriate Cyber Response Plan;

- ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures and to approve the Online Safety Policy and procedures, reviewing its effectiveness e.g., through governors or a governor sub-

committee receiving regular information about online safety incidents and monitoring reports and making use of the UK Council for Internet Safety (UKCIS) guide Online safety in schools and colleges: Questions from the Governing Board;

- ensure that appropriate filters and appropriate monitoring systems are in place, but also consider how 'over-blocking' may lead to unreasonable restrictions on what pupils can be taught in relation to online teaching and safeguarding;

- ensure that the SLT and all staff have an awareness and understanding of the procedures and processes in place to manage filtering and monitoring and how to escalate concerns when identified;

- ensure all governors and trustees receive appropriate training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring in relation to school owned IT devices;

- ensure that the school follows all current online safety advice (including that for online filtering and monitoring) to keep both pupils and staff safe;

- support the school in encouraging parents and the wider community to become engaged in online safety activities;

- have regular reviews with the Online Safety Coordinator/Designated Safeguarding Lead (DSL) and incorporate online safety into standing discussions of safeguarding at governor meetings (including incident logs, adverse monitoring reports, change control logs etc.)

- ensure that where the online safety coordinator is not the named DSL or deputy DSL, there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety as a whole is not compromised;

- work with the Data Protection Officer (DPO), DSL and Principal to ensure a UK GDPR compliant framework for storing data, helping to ensure that child protection is always at the forefront and data protection processes support careful and legal sharing of information;

- check that the trust is making good use of information and support (Annex D - Online Safety which forms part of 'Keeping Children Safe in Education');

- ensure that all staff undertake regular updated safeguarding training, including online safety training in line with advice from the Local Safeguarding Children's Partnerships (LSCP), and that it is integrated, aligned, and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning;

- ensure that appropriate filters and appropriate monitoring systems are in place, but also consider how 'over-blocking' may lead to unreasonable restrictions on what students can be taught in relation to online teaching and safeguarding;

- ensure that the SLT and relevant staff have an awareness and understanding of the provisions in place to manage filtering and monitoring and how to escalate concerns when identified;
- recognise that a one size fits all educational approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed;

- ensure students are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.

1.2 Principal

The Principal has overall responsibility for online safety provision. The day-to-day responsibility for online safety may be delegated to the Online Safety Coordinator or Lead/Designated Safeguarding Lead (DSL).

The Principal; will:

- take overall responsibility for data and data security;

- foster a culture of safeguarding where online safety is fully integrated into academy wide safeguarding;

- oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported;

- ensure that policies and procedures are followed by all staff and other adults working paid or unpaid in the academy;

- undertake training in offline and online safety, in accordance with statutory guidance and relevant Local Safeguarding Partnership recommendations;

- take responsibility for liaising with the Governors in order to achieve their obligations in meeting the DfE digital and technology standards, particularly as they relate to cyber security and filtering and monitoring and ensuring the Governors are regularly updated on progress towards the standards;

- ensure that online safety is appropriately monitored and reviewed by undertaking an annual review of the school's approach to online safety, supported by an annual review of the risk assessment that considers and reflects the risks the children face. We will use appropriate tools for this purpose such as the self-review tool 360o safe or LGfL online safety audit.

- liaise with the DSL on all online-safety issues which might arise and receive regular updates on academy issues and broader policy and practice information;

- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Governors to ensure a Data Protection Act 2018 (DPA) compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information;

- ensure the academy implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;

- be responsible for ensuring that all staff receive suitable training on induction to carry out their child protection and online safety roles (which should include the procedures and processes in place to manage filtering and monitoring and how to escalate

concerns when identified). UKCIS have published an Online Safety Audit Tool which helps mentors of trainee teachers and early career teachers induct mentees and provide ongoing support, development and monitoring;

- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident involving a pupil or an incident which results in an allegation against a member of staff or other adult (see flowchart for dealing with online safety incidents);

- encourage parents/carers to provide age-appropriate supervision for children in their care using the internet including by the use of internet filters which should be used to block malicious websites (usually free but often need turned on. Information for parents/carers will be regularly updated and published on the school website and via newsletters and other publications.

- ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including the risk of children being radicalised;

- take responsibility for formulating the school's Cyber security resilience strategy and Cyber response plan in liaison with the Online Safety Governor and other third party providers.

- ensure the school website meets statutory requirements (see KAHSC guidance on statutory and desirable website features and content for academy schools).

1.3   Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL)

The DSL may delegate certain online safety duties e.g. to the OSL, but not the day-to- day responsibility; this assertion and all quotes below are taken from Keeping Children Safe in Education. Where the online-safety co-ordinator is not the named DSL or deputy DSL, there must be a regular review and open communication between these roles to ensure that the DSL's clear overarching responsibility for online safety is not compromised.

The Designated Safeguarding Lead/Online Safety Lead will:

- take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)

- be the first point of contact for any concerns the wider staff and other adults working in the academy may have in relation to child protection and online safety harmful behaviour e.g., sharing nude or semi-nude images/online challenges or hoaxes and refer to the UKCIS guidance Sharing nudes and semi-nudes: how to respond to an incident and the DfE Guidance Harmful online challenges and online hoaxes

- ensure an effective approach to online safety is in place that empowers the school to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate;

- source innovative ways to promote an awareness and commitment to online safety throughout the academy community with strong focus on parents, who are often appreciative of academy support in this area, but also including 'hard-to-reach' parents;

- liaise with other agencies in line with 'Working together to Safeguard Children' statutory guidance;

- have an understanding of the unique risks associated with online safety (including an understanding of the filtering and monitoring systems and processes in place in the school) and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school and to support other adults in doing so;

- ensure that online safety education is embedded in line with DfE guidance Teaching Online Safety in schools across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World' and the ProjectEVOLVE - Education for a Connected World Resources) and beyond, in the wider school community;

- take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;

- ensure that online safety education is embedded in line with DfE guidance 'Teaching Online Safety in schools' across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in the wider school community;

- work with the Principal, Data Protection Officer, governors, and the trust ICT technical staff to ensure a DPA compliant framework for storing data, helping to ensure that child protection is always at the fore and data protection processes support careful and legal sharing of information;

- keep up to date with the latest local and national trends in online safety;

- review and update this policy and procedures, other online safety documents (e.g., Acceptable Use Agreements) and the strategy on which they are based (in line with policies and procedures for behaviour and child protection) and submit for review on a regular basis to the trustees/governors;

- liaise with academy technical, pastoral, and support staff as appropriate;

- communicate regularly with leadership team and the designated online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs;

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and that these are logged in the same way as any other child protection incident;

- oversee and discuss 'appropriate filtering and monitoring' with governors in order to meet the DfE Filtering and monitoring standards (both physical and technical) and ensure staff are aware of its necessity;

- ensure the DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this as well as to bullying generally;

- facilitate training and advice for staff and others working in the school to ensure that:

- all staff read and understand KCSiE Annex A unless they work in the leadership team or directly with children when they must read and understand KCSiE Part one and Annex B;

- all staff are aware of information relevant to their role in keeping children safe online signposted in KCSiE Annex D

- cascade knowledge of risks and opportunities throughout the organisation;

- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:

  - sharing of personal data;
  - access to illegal/inappropriate materials;
  - inappropriate online contact with adults/strangers;
  - potential or actual incidents of grooming;
  - cyberbullying and the use of social media.

1.4 All Staff

It is the responsibility of all staff to:

- understand that online safety is a core part of safeguarding; as such it is part of everyone's role. Never think that 'someone else will pick it up';

- know who the Designated Safeguarding Lead and Online Safety Lead are;

- read and understand Annex A of 'Keeping Children Safe in Education' unless they work in the SLT or directly with children when they must read and understand Part 1 and Annex B instead;

- read, understand, and help promote the Trust's Online Safety Policy and procedures in conjunction with the Child Protection and other related trust and academy policies and procedures;

- read, sign, and follow the Trust's Staff Acceptable Use Agreement and staff Code of Conduct;

- be aware of online safety issues related to the use of mobile technology e.g., phones, cameras and other hand-held devices and follow Trust procedures in relation to these devices;

- ensure the security of their username and password for the academy network, not allow other users to access the systems using their log on details and immediately report any suspicion or evidence that there has been a breach of security. Passwords will be changed on a regular basis and at least every six months;

- should understand (via training and other means) the different roles and responsibilities for the filtering and monitoring of online systems and expectations of them in their role, including for their own online activities on any device using the school network or on school-owned devices using any network;

- record online safety incidents in the same way as any child protection incident and report incidents to the DSL/OSL in accordance with academy procedures;

- notify the DSL/OSL if policy does not reflect practice in the academy and follow escalation procedures if concerns are not promptly acted upon;

- identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise;

- whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (check what appropriate filtering and monitoring processes are in place);

- carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g., fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law;

- prepare and check all online source and resources before using in the classroom;

- encourage student to follow their Acceptable Use Agreement, regularly remind them about it and enforce Trust sanctions where there is a breach of the Agreement;

- notify the DSL/OSL of new trends and issues before they become a problem;

- take a zero-tolerance approach to bullying and low-level sexual harassment either offline or online;

- receive and act upon regular updates from the DSL/OSL and have a healthy curiosity for online safety issues;

- model safe, responsible, and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the academy and the professional reputation of all staff;

- ensure that any digital communications with studnets are on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones or social media messaging or posts.

1.5   PSHE/RSHE Lead(s)

Responsibilities of PSHE/RSHE Leads include:

- all as listed in the 'all staff' section above;

- ensuring that consent, mental wellbeing, healthy relationships and staying safe online is embedded into the PSHE/Relationships education, relationships, and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of the students' online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their students' lives (KCSiE);

- complementing the computing curriculum which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating

risks that students face. This includes how to use technology safely, responsibly, respectfully, and securely, and where to go for help and support when the pupil has concerns about content or contact on the Internet or other online technologies;

• working closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches, and messages within PSHE/RSHE.

1.6 Computing/Subject Lead(s)

Responsibilities of the Computing Lead include:

• all as listed in the 'all staff' section above;

• the overseeing delivery of the online safety element of the computing curriculum in accordance with the national curriculum;

• working closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches, and messages within computing;

• collaboration with technical staff and others responsible for ICT use in academy to ensure a common and consistent approach, in line with Acceptable Use Agreements.

1.7 Network Manager/Technical staff/IT Provider Staff

Responsibilities of the Network Manager/ICT Technicians include:

• all as listed in the 'all staff' section above;

• supporting Governors and SLT in achieving the DfE digital and technology standards;

• supporting SLT in the formulation of a Cyber Security resilience strategy and appropriate Cyber response plan as outlined in the DfE Cyber security standards;

• reporting any online safety related issues that arise through external monitoring reports, to the DSL/OSL in the first instance;

• reporting any online safety related issues that arise, to the DSL/OSL in the first instance;

• keeping up to date with the trust's Online Safety policy and technical information to effectively carryout their online safety role and to inform and update others as relevant;

• working closely with the DSL/OSL/DPO to ensure that school systems and networks reflect Trust policy;

• ensuring that the above stakeholders understand the terms of existing services and how any changes to these systems (especially in terms of access to personal and sensitive records/data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.) might affect the system functions and safety online;

• supporting and providing advice on the implementation of 'appropriate filtering and monitoring' in order to meet the school's obligations outlined in the DfE Filtering and Monitoring standards;

- ensuring that users may only access the trust's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;

- ensuring that the trust's ICT infrastructure is secure and is not open to misuse or malicious attack e.g., keeping virus protection up to date;

- ensuring that access controls/encryption exist to protect personal and sensitive information held on trust-owned devices;

- monitoring the use of the network/ remote access/email and social media presence and that any misuse/attempted misuse is reported to the DSL/OSL in line with trust policy;

- ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a cyber-attack or other disaster and to complement the business continuity process and cyber response plan;

- maintaining up-to-date documentation of the trust's online security and technical procedures;

- working with the Principal to ensure the academy website meets statutory DfE requirements;

- reporting online safety issues that come to their attention in line with trust policy.

1.8 Data Protection Officer (DPO)

The DPO will be familiar with references to the relationship between data protection and safeguarding in key DfE documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools'.

The Data Protection Act 2018 and UK GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe and promoting their welfare. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with DPA 2018. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

Other responsibilities of the DPO include:

- working with the DSL, Principals, Trustees and Governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above;

- ensuring that all access to safeguarding data is limited as appropriate, monitored, and audited.

1.9 Volunteers and contractors

The key responsibilities of volunteers and contractors are to:

- read, understand, sign, and adhere to any Acceptable Use Agreement issued by the trust;
- report any concerns, no matter how small, to the DSL/OSL without delay;
- maintain an awareness of current online safety issues and guidance;
- model safe, responsible, and professional behaviours in their own use of technology.

1.10 Students

Taking into account their age and level of understanding, the key responsibilities of students are to:

- use the trust's ICT systems in accordance with the age-appropriate student Acceptable Use Agreement – see Appendix D or E, which they and/or their parents will be expected to sign before being given access to the academy systems. As with consent on data (privacy notices) Agreements must be written in terms the EYFS/KS1 child can understand;

- ensure the security of their username and password for the academy system, 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;

- understand the importance of reporting abuse, misuse or access to inappropriate materials including those involving hoaxes and on-line challenges and know how to do so;

- know what action to take if they or someone they know feels worried or vulnerable when using online technology;

- understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of the academy and realise that the trust's acceptable use agreements cover their actions outside of the academy, including on social media;

- know and understand academy procedures on the use of mobile phones, digital cameras, and other digital devices;

- know and understand trust procedures on the taking/use of images and on cyberbullying/sharing nude and semi-nude images;

- understand that the school is able to, and will, impose filtering rules and will monitor the use of school owned digital devices for inappropriate access to, or downloads from, websites. Beaches may lead to sanctions as described in the School Behaviour Policy and procedures and, in some cases, may involve the Police;

- understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at the academy if there are problems.

1.11 Parents

Parents play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The trust will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature.

The key responsibilities for parents are to:

- support the trust in promoting online safety which includes the students' use of the Internet and the academy's use of photographic and video images;

- work with and support the school when issues or concerns are identified which are as a result of the school's filtering and monitoring procedures and processes;

- read, sign, and promote the student Acceptable Use Agreement and encourage their child to follow it;

- consult with the academy if they have any concerns about their child's and others' use of technology;

- promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology (including on social media) by ensuring that they themselves do not use the Internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;

- support the trust's approach to online safety by not uploading or posting to the Internet any images or details of others without permission and refraining from posting pictures, video or text that could upset, offend, or threaten the safety of any member of the trust community or bring the trust into disrepute.

2.   TEACHING AND LEARNING

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk known as the 4Cs:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.

- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Strong links between teaching online safety and the curriculum (see also Roles above) are the clearest in:

- Personal, Social and Health Education (PSHE)
- Relationships education, relationships, and sex education (RSE) and health
- Computing/ICT
- Citizenship

It is, however, the role of all staff to identify opportunities to thread online safety through all academy activities, both outside the classroom and within the curriculum, supporting subject lead staff and making the most of unexpected learning opportunities as they arise.
We will make reference to the DfE guidance 'Teaching online safety in schools' and the UKCIS guidance 'Education for a Connected World'.

Whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff will encourage sensible use, monitor (either physically; by the use of internet and web access software or via the use of active/proactive technology monitoring services) what pupils are doing and consider potential dangers and the age appropriateness of websites.

Whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc.) in the academy or setting as homework tasks, all staff will encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g., fake news), age-appropriate materials and signposting, and legal issues such as copyright, plagiarism and data law.

We recognise that online safety and broader digital resilience must be included throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND students) are used as an opportunity to assess the key areas of self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership.

2.1 How internet use enhances learning

This academy:

• has a clear, progressive online safety education programme as part of the Computing/ICT/PSHE curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the students concerned and include those to:

- STOP and THINK before they CLICK;

- develop a range of strategies to evaluate and verify information before accepting its accuracy;

- be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;

- know how to narrow down or refine a search;

- [for older students] understand how search engines work and to understand that this affects the results they see at the top of the listings;

- understand acceptable behaviour when using an online environment/email, i.e., be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

- understand how photographs can be manipulated and how web content can attract unwanted or inappropriate attention;

- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs, and videos and to know how to ensure they have turned-on privacy settings;

- understand why they must not post pictures or videos of others without their permission;

- know not to download any files – such as music files – without permission;
- have strategies for dealing with receipt of inappropriate materials;

- [for older students] understand why and how some people will 'groom' young people for sexual or extremist ideology reasons;

- understand the impact of cyberbullying, sharing inappropriate images and trolling and know how to seek help if they are affected by any form of online bullying;

- know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e., parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;

- will remind students about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the academy or when they log on to the academy's network;

- ensures staff model safe and responsible behaviour in their own use of technology during lessons;

- ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright/intellectual property rights;

- ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop- ups; buying online; online gaming/gambling etc.

2.2   Students with additional needs

We use a wide range of strategies to support children with additional needs who might need extra support to keep themselves safe, especially online.

- Sensitively check students' understanding and knowledge of general personal safety issues using reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.

- Apply rules consistently to embed understanding.

- Communicate rules clearly to parents and seek their support in implementing school rules at home. Working with parents and sharing information with them is relevant to all children, but this group especially.

- Careful explanations about why rules might change in different situations i.e., why it is ok to give your name and address to an adult if you are lost in town, but not when using the Internet.

- Consistent use of cause and effect linking the rules to consequences teaching realistic and practical examples of what might happen if… without frightening students.

2.3   Remote Education

While the remote education temporary continuity direction which required schools to provide remote education to students where their attendance would be contrary to government guidance or legislation in force at the time has ended, the DfE expects schools to continue to maintain their capabilities to deliver high quality remote education for the next academic year.

This is because government public health advice locally or nationally may require a class, group, or a small number of students to self-isolate, and all such students not physically unwell should have access to remote education as soon as reasonably practicable, which may be the next school day.

When this academy is required to provide it, remote education should be equivalent in length to the core teaching students would receive in the academy and should include recorded or live direct teaching time, as well as time for students to complete tasks and assignments independently. As a minimum we will provide 3 hours/day on average across the cohort in Key Stage 1, with less for younger children, and 4 hours/day in Key Stage 2, and 5 hours/day on average across the cohort for Key Stages 3 and 4.

To ensure business continuity, thorough emergency preparedness, continuity of education and safeguarding arrangements, and to prevent harms, trustees may decide to implement remote learning provision in any kind of local or national emergency situation that prevents students or staff attending to statutory schooling.

In developing our remote education provision, we have:

- Selected the Google Classroom digital platform to use consistently across the academy to allow interaction, assessment, and feedback with procedures in place to ensure staff are trained and confident in its use. This enables us to provide online video lessons recorded by teaching staff and high-quality lessons developed by external providers as well as monitored methods of communication.

- Identified ways to discover and overcome barriers to digital access for students e.g., forms or other survey methods, distributing school-owned laptops, securing appropriate internet connectivity solutions, providing printed resources, such as textbooks and workbooks, to structure learning, supplemented with other forms of communication to keep students on track or answer questions about work.

- Ensured that trust-owned devices distributed for the purpose of access to remote education will always include appropriate safeguarding controls and support to help

children and families, and staff use them safely, including information about physically healthy computing e.g., posture, the teaching and learning environment, sleep.

- Ensured we can teach a planned and well-sequenced curriculum so that knowledge and skills are built incrementally.

- Published on the academy website up-to-date information about what is intended to be taught and practised in each subject so that students can progress through the curriculum.

- Put systems in place for checking, daily, whether students are engaging with their work, so we can work with families to rapidly identify effective solutions where engagement is a concern.

- Identified a named senior leader, Barry Simpson, with overarching responsibility for the oversight of the quality, delivery, and safety of remote education.

- Considered issues that specific individuals or groups of students may have engaging with remote education due to their age, stage of development, special educational needs, or disability e.g., where this would place significant demands on parents' help or support, ensuring that the teachers best placed to know how the students' needs can be most effectively met to ensure they continue to make progress, work with families to deliver an ambitious and appropriate curriculum.

- Sought to demonstrate that we understand the requirement for schools under the 2014 Children and Families Act to use our best endeavours to secure thespecial educational provision called for by the students' special educational needs remains in place.

- Identified potential personal, professional, and children's safeguarding issues associated with the provision of remote education; put in place hardware, software, procedures, and training to reduce the risk of harm to the adults, children, and young people exposed to it; and ensured the risks are being addressed in a consistent and ongoing way through the curriculum (see below).

- Reviewed and updated as necessary relevant policies, procedures, and supporting documents like our Acceptable Use Agreements in light of remote education provision to ensure that they remain appropriate and useful for keeping the adults, children, and young people exposed to it safe online.

In the provision of remote education this school undertakes to:

- Set meaningful and ambitious work each day in an appropriate range of subjects

- Transfer into remote education what we already know about effective teaching in live classrooms by:

  - providing frequent, clear explanations of new content, delivered by a teacher or through high-quality curriculum resources
  - providing opportunities for interactivity, including questioning, eliciting and reflective discussion
  - providing scaffolded practice and opportunities to apply new knowledge
  - enabling students to receive timely and frequent feedback on how to progress, using digitally facilitated or whole-class feedback where appropriate
  - using assessment to ensure teaching is responsive to students' needs and addresses any critical gaps in students' knowledge

- avoiding an over-reliance on long-term projects or internet research activities

• Ensure leaders and teachers are appropriately signposted to the Get help with remote education support package, relevant peer-to-peer advice and training available through the EdTech Demonstrator programme , and guidance on supporting pupils and students with SEND to access remote education.

• Notify their social worker (if they have one) when a vulnerable pupil is asked to self-isolate and agree with the social worker the best way to maintain contact and offer support.

• Review and self-assess the our remote education offer regularly using the DfE review your remote education provision tool or similar.

• Continue to record attendance accurately in the register for students who are receiving remote education in line with any current government guidance on it.

• Carry out an annual review of the Trust's approach to online safety, supported by an annual risk assessment that considers and reflects the risks the students that attend this academy face using a tool like the 360 safe website.

We recognise that there are additional safeguarding risks to students associated with them spending more time online than before the global pandemic, both in their leisure time and to be able to access remote education. There may also be risks from or to the people they live with during live video link work and staff are expected to plan accordingly and seek advice from the OSL/DSL as necessary. The student Acceptable Use Agreement includes expected conduct during remote education activities.

We recognise that there are additional safeguarding risks to staff as well, especially those facilitating remote learning via live video links that may also impact other people in their household or community. The Staff Code of Conduct sets out expected good remote education practice.

We will follow relevant government online safeguarding guidelines and make use of recommended technical tools and guides signposted there to help us deliver remote education safely.

In addition to the updated codes of conduct, staff, students (or due to their age and ability, the adults supporting them), parents, carers, and to some degree, virtual or in- person visitors using online technology for education purposes or school business are expected to:

Check security and privacy settings e.g.:

• Adjust privacy and safety settings on all devices, in apps and other online places to control what personal data is shared.

• Review the security settings on 'smart' devices and change any default, weak or guessable passwords.

• Set up two-factor authentication if devices are capable or available.

• Regularly update devices or apps used by the academy or work to improve security.

- Think about physical privacy when appearing live online e.g., adult supervision of children at home, appropriate clothing, distractions like noise and interruptions, what other people nearby can hear.

Act regarding unsuitable content e.g.:

- Prevent unwanted content from appearing i.e. set filters and parental controls on home broadband and mobile networks and not disable or bypass them (the UK Safer Internet Centre has advice on how).

- Block unsuitable contact (with support as necessary)

- Report harmful activity, to the website, platform or app, a trusted adult, and the DSL. Report Harmful Content to Safer Internet UK if not satisfied with the result of a report to a service provider.

Protect against fraud e.g.

- Beware of fraud and scams online including phishing emails and text messages and use appropriate cyber security and "stop, challenge, protect" information to avoid becoming a victim.

- Forward suspicious emails to reportphishing@apwg.org, using the "Forward as attachment" option if possible to enhance tracking to the Anti-Phishing Working Group for analysis.

- Never give out personal information to websites or in response to emails/text messages not recognised or trusted.

- Report being scammed, defrauded, or experiencing cyber-crime to Action Fraud, the UK's national reporting centre.

Check the Facts e.g.: use the SHARE checklist to make sure they are not contributing to the spread of harmful content e.g.

Stay physically and mentally healthy online e.g.:

- Take regular breaks from online activities and use tools like Apple's Screen Time, Google's Family link, Xbox One, PlayStation 4, Nintendo Switch if necessary to manage screen time, especially if feeling overwhelmed, or in physical discomfort.

- Take notice of any guidance the academy provides on supporting children's mental health and wellbeing or that of staff as well as practical guidance on making the home environment a good and safe one to learn in with school adopting a sensitive appreciation for people's different home circumstances and what is reasonable.

Staff are also expected to:

- Provide information about their temporary home working environment insofar as it might impact on their physical health, or the safeguarding of learners or their own household.

- Act appropriately on feedback and use any necessary online or cyber tools provided.

- Provide information about the technology they use at home to get online i.e., to ensure compatibility with Trust systems, especially cyber security measures involved in accessing sensitive data like medical, behaviour or performance information on school servers remotely.

- Implement relevant guidance on safe teaching and pastoral care from their home e.g., what is in the background of recorded or live streams, what is visible on shared screens, what can be heard by others in a household etc.

- Pay special attention to how they protect personal data at home.

- Report to their line manager any issues or concerns they may have either about their personal safety or that of a student.

- Keep talking about staying safe online, which we can do by:

  - Ensuring staff have the tools to promote a healthy balance between the positive and negative aspects of life online.

  - Signposting parents and carers to tools to explain and reduce risks and help them talk to their child.

  - Reiterating behaviour expectations and ways to handle and report problems, especially encouraging children to speak to a trusted adult if they come across content online that makes them uncomfortable.

  - Supporting critical thinking and promoting resources like Parent Zone's guide and Childnet's advice and top tips which provide ways parents and carers can help their child develop these skills.

3.   HANDLING ONLINE SAFETY CONCERNS AND INCIDENTS

Our staff recognise that online safety is only one element of the wider safeguarding agenda as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns will be handled in the same way as any other child protection concern. Early reporting to the DSL/OSL is vital to ensure that the information contributes to the overall picture or highlights what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

Procedures for dealing with online safety, concerns and incidents are detailed in the following Policies:

- Child Protection Policy and procedures
- Child on child (aka Peer on peer abuse) policy and procedures
- Whole School Behaviour   policy and   procedures   (includes   anti-bullying procedures)
- Acceptable Use Agreements
- Prevent Risk Assessment

- Data Protection policy, agreements, and other documentation (e.g., privacy statement, consent forms for data sharing image use etc.)

We are committed to taking all reasonable precautions to ensure online safety but recognise that incidents will occur both inside and outside school. All members of the school community are encouraged to report issues swiftly to school staff so that they can be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL/OSL on the same day wherever possible or, if out of school, the following school day.

Any concern/allegation about misuse by staff or other adult in school will always be referred directly to the Principal unless the concern is about the Principal, in which case, the complaint will be directed to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline. Call 0800 028 0285 or email: help@nspcc.org.uk.

The Trust will actively seek support from other agencies as needed (i.e., Local Authority Safeguarding Hub, UK Safer Internet Centre's Professionals' Online Safety Helpline (03443814772), NCA CEOP, Cumbria Police Prevent Officer, Cumbria Police, Internet Watch Foundation (IWF)). We will inform parents of online safety incidents involving

their child and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or is considered illegal. See Sections below for procedures for dealing with sharing nude and semi-nude images, upskirting and online bullying.

- In this school there is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions.

- All members of the Trust community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

- The Online Safety Coordinator will record all reported incidents and actions taken in the academy Online Safety incident log and other in any relevant areas e.g., bullying or child protection log.

- The Designated Safeguarding Lead will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection policy and procedures for dealing with concerns.

- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.

- The academy will inform parents of any incidents or concerns as and when required.

- After any investigations are completed, the academy will debrief, identify lessons learnt and implement any changes required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub and escalate the concern to the Police.

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour/disciplinary procedures. It is important that, where necessary, members of the academy community are made aware that incidents have been dealt with.

3.1   Sharing nude and semi-nude images

Where incidents of the sharing of nude and semi-nude images via the internet or mobile phone by those under the age of 18 are discovered , we will refer to the UK Council for (UKCIS) guidance 'Sharing nude and semi-nude images'. A copy of this document is

available from the school office. Where one of the parties is over the age of 18, we will refer to it as child sexual abuse.

All staff and other relevant adults have been issued with a copy of the UKCIS overview document (Sharing nudes and semi-nudes: how to respond to an incident) in recognition of the fact that it is generally someone other than the DSL or OSL who will first become aware of an incident. Staff, other than the DSL, must not attempt to view, share, or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

The Trust will ensure that a whole-school approach is embedded so that children and young people understand what 'online sexual harassment' is and instances of sexual harassment are prevented from occurring. Within this approach victims will be empowered to report their concerns and feel reassured that they are being taken seriously and that they will be supported and kept safe. It is important to understand that whilst the sharing of nude and semi-nude images is illegal, the Trust will create a culture to support and encourage students to discuss, with staff, situations where they have made a mistake or have a problem with this issue and that all victims are reassured that they are being taken seriously when they make a report and that they will be supported and kept safe.

The UKCIS advice outlines how to respond to an incident of nudes and semi-nudes being shared including:

- risk assessing situations;
- safeguarding and supporting children and young people;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents and carers

The types of incidents which this advice covers are:

-     a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18;
-     a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18;
-     a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.

3.2   Upskirting

All staff are aware that 'upskirting' (taking a photo of someone under their clothing) is now a criminal offence, but that students should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue. If staff or other adults become aware of an incident of 'upskirting', the issue must be reported to the DSL as soon as possible.

3.3   Online bullying

Online bullying (also known as cyberbullying) will be treated in the same way as any other form of bullying and the Whole School Behaviour policy and procedures will be

followed in relation to sanctions taken against the bully. It is important not to treat online bullying separately to offline bullying and to recognise that some bullying will have both online and offline elements. Support will be provided to both the victim and the perpetrator. In some cases, it may be necessary to inform or involve the Police.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming, or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are several statutory obligations on schools in relation to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

-     every school must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the school's Behaviour Policy which must be communicated to all students, school staff and parents;

-     gives Principals the ability to ensure that students behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside the Trust (such as online or via text) is reported to the Trust, it will be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If Trust staff feels that an offence may have been committed, they should seek assistance from the Police.

All staff have a role in implementing our behaviour policy and our procedures for tackling cyberbullying as follows, and are encouraged to use Resources | Childnet which offers guidance and practical advice (select the topic online bullying):

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the Whole School Behaviour Policy and procedures.

- There are clear procedures in place to support anyone in the Trust community affected by cyberbullying.

- All incidents of cyberbullying reported to the Trust will be recorded.

- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.

- Students, staff, and parents will be advised to keep a record of the bullying as evidence.

- The Trust will take steps to identify the bully, where possible and appropriate. This may include examining academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Students, staff, and parents will be required to work with the Trust to support the approach to cyberbullying and the Trust's online safety ethos.

- Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at the academy for the user for a period of time. Other sanctions for students and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.

- Parents of students will be informed.

- The Police will be contacted if a criminal offence is suspected.

3.4   Harmful online challenges or hoaxes

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

If staff are confident children and young people are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed by either the DSL or a senior leader in school. Careful consideration will be given on how best to do this, and it may be appropriate to offer focussed support to a particular age group or individual children at risk. We will take account of the fact that even with real

challenges, many children and young people may not have seen it and may not be aware of it and will carefully weigh up the benefits of institution-wide highlighting of the potential harms related to a challenge against needlessly increasing children and young people's exposure to it.

Where staff become aware of a potentially harmful online hoax or challenge, they will immediately inform the Designated Safeguarding Lead who will take the appropriate action either with the child concerned or with the wider group where the incident involves more than one child.

Where the DSL considers it necessary to directly address an issue, this can be achieved without exposing children and young people to scary or distressing content. In the response, we will consider the following questions:

• is it factual?
• is it proportional to the actual (or perceived) risk?
• is it helpful?
• is it age and stage of development appropriate?
• is it supportive?

A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

We will carefully consider if a challenge or scare story is a hoax. Generally speaking, naming an online hoax, and providing direct warnings is not helpful. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children and young people. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children and young people's exposure to distressing content.

Evidence from Childline shows that, following viral online hoaxes, children and young people often seek support after witnessing harmful and distressing content that has been highlighted, or directly shown to them (often with the best of intentions), by parents, carers, schools, and other bodies. In this respect, staff will be mindful of the advice provided by the UK Safer Internet Centre which provides guidance on dealing with online hoaxes or challenges.

In any response, reference will be made to the DfE guidance 'Harmful online challenges and online hoaxes'

3.5   Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in 'Keeping Children Safe in Education' and separate guidance exists on this issue 'Sexual violence and sexual harassment between children in schools and colleges'. All staff are aware of this guidance.

We take all forms of sexual violence and harassment seriously and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures.

3.6   Misuse of Trust technology (devices, systems, networks, or platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of Trust networks, connections, internet connectivity and devices, cloud platforms and social media (both when on the academy site and outside of the academy).

These rules are defined in the relevant Acceptable Use Agreements as provided to students, staff, trustees and governors.

Where students contravene these rules, the Whole School Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the Trust disciplinary procedures.

The Trust reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto trust property.

3.7   Social media incidents

See also Section 9 below. Social media incidents are governed by Acceptable Use Agreements. Breaches will be dealt with in line with these procedures, the Whole School Behaviour policy and procedures (for students) and the staff Code of Conduct/Disciplinary procedures (for staff and other adults).

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by an identifiable member of the academy community, we will request that the post be deleted and will expect this to the actioned promptly.

Where an offending post has been made by a third party or is anonymous, the Trust may report it to the hosting platform, the Police or may contact the Professionals' Online Safety Helpline (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

4.   DATA PROTECTION AND DATA SECURITY

All students, staff, trustees, governors, parents, and other adults working in or visiting Trust academies are bound by the Trust's Data Protection Policy and procedures a copy of which is available from trust offices.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' which the DPO and DSL will seek to apply.

The DPO and Principals will work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always the primary consideration and data protection processes support careful and legal sharing of information. The Data Protection Act 2018 does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with the DPA. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

All students, staff, trustees, governors, volunteers, contractors, and parents are bound by the Trust's Data Protection policy and procedures.

4.1   Maintaining Information Systems Security

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g., the downloading of large files or viewing sporting events during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For staff, flouting the Trust's Acceptable Use Agreement may be regarded as a reason for dismissal.

- Workstations should be secured against user mistakes and deliberate actions.

- Servers will be located securely and physical access restricted.

- The server operating system is secured and kept up to date.

- Virus protection for the whole network is installed and current.

- Access by wireless devices will be proactively managed.

Wide Area Network (WAN) security issues include:

- Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between academies.

- Decisions on WAN security are made in partnership between the Trust and its network provider.

The following statements apply in our trust:

- The security of the Trust's information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.

- Personal data sent over the internet or taken off site will be encrypted.

- Portable media may not be used without specific permission followed by an anti-virus/malware scan.

- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the Trust's network will be regularly checked.

- The Trust Network manager will review system capacity regularly.

- Use of user logins and passwords to access the trust network will be enforced – see Section 6.2 below.

The Trust's broadband and online suppliers are Virtue.

The Data Protection Officer and Principals work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always put first, and data protection processes support careful and legal sharing of information.

4.2   Password Security

We will ensure that the Trust's networks are safe and secure as is reasonably possible and that users can only access data to which they have right of access; no user is able to access another's files without permission (or as allowed for monitoring purposes within the Trust's procedures); access to personal data is securely controlled in line with the Trust's personal data procedures; logs are maintained of access by users and of their actions while users of the system.

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the Network Support Team. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

Users will change their passwords every 90 days.

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This will apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the Trust's password security procedures:

•   at induction;
•   through the Trust's Online Safety policy and procedures;
•   through the Acceptable Use Agreement.

Students will be made aware of the Trust's password security procedures:

•   in Computing/ICT and/or Online Safety lessons;
•   through the Acceptable Use Agreement.

The following rules apply to the use of passwords:

•   passwords must be changed every 90 days;
•   the last four passwords cannot be re-used;
•   the password will be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
•   the account should be "locked out" following six successive incorrect log-on attempts;
•   temporary passwords e.g., used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
•   passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);
•   requests for password changes should be authenticated by to ensure that the new password can only be passed to the genuine user.

The "master/administrator" passwords for the Trust ICT system, accessible only be the Network Manager and Senior Network Technician, are kept in a secure place. Where an academy has a "master/administrator password for the academy's ICT system only the Principals will have access to this and they will be kept in a secure place.

Audit/Monitoring/Reporting/Review:

The Network Manager and/or Senior Network Technician will ensure that full records are kept of:

• User Ids and requests for password changes;
• User log-ons;
• Security incidents related to this policy and procedures.

In the event of a serious security incident, the Police may request and will be allowed access to passwords used for encryption.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by the DPO at regular intervals.

5. ELECTRONIC COMMUNICATIONS

5.1 Managing Email

Our general principles for email use are as follows:

• Students may only use approved email accounts for Trust purposes.

• Students must immediately tell a designated member of staff if they receive an offensive email or one which upsets or worries them.

• Students must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.

• Whole-class or group email addresses will be used in primary schools for communication outside of the Trust.

• Whole class or group email addresses will be used with the exception of students in Year 6 and above will be provided with individual school email addresses for educational use.

• Staff will only use official Trust provided email accounts to communicate with students and parents, as approved by the leadership team. Any deviation from this must be agreed with the DSL/Principal.

• Any digital communication between staff and students or parents (email, chat, online educational resource etc.) must be professional in tone and content. These communications may only take place on official (monitored) Trust systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (if by a staff member).

• Staff are not permitted to use personal email accounts during school hours or for professional purposes.

• Students and staff are not permitted to use the Trust's email system for personal use and should be aware that all use is monitored, their emails may be read, and the same

rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the Trust into disrepute or compromise the professionalism of staff.

- Users must immediately report to the DSL the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information must not be posted on the Trust and academies websites and only official email addresses will be used to identify members of staff.

- Spam, phishing, and virus attachments can make email dangerous. The Trust's ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

5.2 Emailing personal, sensitive, confidential, or classified information

Staff or student personal data must be encrypted prior to being sent via email.

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;

- Where your conclusion is that the Trust email must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by email;

  - Exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information;
- Verify (by phoning) the details of a requestor before responding to email requests for information;
- Do not copy or forward the email to any more recipients than is necessary.

  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);

  - Send the information as an encrypted document attached to an email;

  - Provide the encryption key or password by a separate contact with the recipient(s) e.g., by telephone or in writing;

  - Do not identify such information in the subject line of any email;

- Request confirmation of safe receipt.

5.3 Zombie accounts

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

•   Ensure that all user accounts are disabled once the member of the academy has left;

•   Prompt action on disabling accounts will prevent unauthorised access;

•   Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days).

Staff will refer to further advice available at IT Governance as necessary.

6.   Trust Websites

The Trust's websites are a key public-facing information portal for the academy communities (both existing and prospective stakeholders) with a key reputational value. Michaela Dockray has day to day editorial responsibility for online content published by the academy on the academy website and will ensure that content published is accurate and appropriate. The academy website is managed by/hosted by Design Works.

The DfE has determined information which must be available on a school website. 'What academies, free schools and colleges should publish online'.

Where other staff submit information for the website, they are asked to consider the following principles:

•   The contact details on the website are the academy address, email, and telephone number. Staff, trustees, governors, or students' personal information are not published.

•   Email addresses will be published carefully online, to avoid being harvested for spam (e.g., by replacing '@' with 'AT').

•   The academies' websites will comply with the Trust's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.

•   Where student work, images or videos are published on the website, their identities are protected, and full names are not published (remember also not to save images with a filename that includes a student's full name).

7.   USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, students and parents need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The

academies will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the Trust agreement form when their child joins the academy. This is a once in an academy lifetime consent. Parents are required to inform the academy if their consent changes.

- We seek consent for the publication of images from students.

- When we publish images or video, we will inform student and parents before publishing, so they have a chance to object as is their legal right under DPA 2018.

- We do not identify students in online photographic materials or include the full names of students in the credits of any published academy produced digital materials. Photo file names/tags do not include full names to avoid accidentally sharing them.

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Staff are governed by their contract of employment, the staff Code of Conduct and sign the Trust's Acceptable Use Agreement. This includes a clause on the use of mobile phones/personal equipment for taking pictures of students.

- The academies block/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

- Staff are permitted to take digital/video images to support educational aims, but must follow Trust procedures concerning the sharing, distribution, and publication of those images. Those images will only be taken on Trust equipment. No member of staff will ever use their personal phone to capture photos or videos of students.

- Staff will ensure that when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute.

- Digital images/videos are stored on the trust network in line with the retention schedule of the Trust's Data Protection Policy.

- Students are taught about how images can be manipulated in their online safety education programme and are taught to consider how to publish for a wide range of audiences which might include governors, parents, or younger children as part of their ICT scheme of work;

- Students are taught that they should not post images or videos of others without their consent. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or academy. We teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.

- Staff and parents are regularly reminded about the importance of not sharing without consent, due to child protection concerns (e.g., children looked-after often have restrictions for their own protection) data protection, religious or cultural reasons or simply for reasons of personal privacy.

- If specific student photos (not group photos) are used on the academy website, in the prospectus or in other high-profile publications the academy will obtain individual parental or pupil consent for its long-term use. (for more information see KAHSC Safety Series: General G21 – The Use of Images when Working with Children and the KAHSC Model Consent Form - trips images and pain relief).

- A student's work can only be published with the consent of the student and parents. We will seek the consent of the student first and then, if necessary, the parents.

8. CLOUD PLATFORMS

This Trust adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies' and our Data Protection Policy and procedures includes the use of Cloud services.

For online safety, basic rules of good password management, expert administration and training is used to keep staff and students safe and to avoid incidents. The DPO and Network Manager will analyse and document systems and procedures before they are implemented and regularly review them.

The following principles apply:

- Privacy statements inform parents and children when and what type of data is stored in the cloud.

- The DPO approves new cloud systems, what may or may not be stored in them and by whom on the basis of a data protection impact assessment (DPIA).

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that student data is not shared by mistake. Open access or widely shared folders are clearly marked as such.

- Students and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.

- Student images/videos are only made public with parental consent.

- Only Trust-approved platforms are used by students or staff to store student work.
- All stakeholders understand the difference between consumer and education products (e.g., a private Gmail account or Google Drive and those belonging to a managed educational domain).

9. SOCIAL MEDIA

9.1 Managing social networking, social media, and personal publishing sites

The Trust operates on the principle that if we don't manage our social media reputation, someone else will. Online reputation management is about understanding and managing our digital footprint (everything that can be seen or read about the Trust online). Negative

coverage almost always causes some level of disruption and can result in distress to individuals.

We therefore manage our social media footprint carefully to know what is being said about the school and in order to respond to criticism and praise in a fair, responsible manner.

The academies have an official Facebook/Twitter/Instagram account which is managed by the individual academies and will respond to general enquiries about the academy, but we ask parents not to use these channels to communicate about their children or other personal matters.

Email is the official electronic communication channel between parents and the school, and between staff and student and we use Office 365 to facilitate this securely.

While we welcome communication about and with us from within and outside our school community online using our social media accounts they must never be used to communicate with us about personal or private matters, including over any private messaging service operated by such social media providers.

Staff, students', and parents' social media presence:

Social media is a fact of modern life and, as a Trust, we accept that many parents, staff, and students will use it. However, as stated in the Acceptable Use Agreements and our Whole School Behaviour policy and procedures we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are, or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise derogatory or inappropriate or which might bring the Trust, student body or teaching profession into disrepute. This applies to both public pages and to private posts e.g., parent chats, pages, or groups.

If parents have a concern about their child's academy, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the Trust's complaints procedure (available via the website) should be followed. Sharing complaints on social media is unlikely to help resolve the matter but can cause upset to staff, students, and parents, also undermining staff morale and the reputation of the Trust/academy.

Many social media platforms have a minimum age of 13 but the Trust deals with issues arising on social media with students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. However, the Trust accepts that there is a balance between not encouraging underage use whilst at the same time needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. However, children will often learn most from the models of behaviour they see and experience. Parents can best support this by talking to their children about the apps, sites, and games they use, with whom, for how long, and when (late at night is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Students are not allowed1 to be 'friends' with or make a 'friend request2' to any staff, trustees, governors, volunteers or regular school contractors or otherwise communicate via social media. Students are discouraged from 'following' staff, trustees, governors, volunteers, or regular contractors' public accounts (e.g., following a staff member with a public Instagram

account). However, we accept that this can be difficult to control. This, however, highlights the need for staff to remain professional in their private lives. Staff must not accept friend or follower requests from students or students on social media, messaging sites or apps.

Staff are reminded that they should not bring the Trust or profession into disrepute and the best way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. Staff must never discuss the Trust or its stakeholders on social media and ensure that their personal opinions are not attributed to the trust. The following principles apply:

- The Trust will take steps to control access to social media and social networking sites. over school networks, on school-owned devices, and on social media or other online accounts we control.

- Appropriate guidance or signposting will be provided for pupils, parents, governors, staff, and volunteers about Social Media and how to use it safely - NCSC.GOV.UK, Social Media - UK Safer Internet Centre, and Social media and online safety | NSPCC Learning.

- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, academy attended, IM and email addresses, full names of friends/family, specific interests, and clubs etc.

- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the leadership team before using social media tools in the classroom.

- Staff official blogs will be password protected and run from the Trust/academy website with approval from the leadership team. Members of staff are advised not to run social network spaces for student use on a personal basis.

- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the academies where possible.

- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

- Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- All members of the Trust community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory.

- Steps will be taken in line with guidance on How schools and parents can spot and tackle online abuse of teachers - The Education Hub (blog.gov.uk).
- Newsgroups will be blocked unless a specific use is approved.

- Concerns regarding a student's use of social networking, social media, and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the Staff Acceptable Use Agreement – see Appendix F.

- Further guidance can be found in the document 'Safe Use of Facebook and Other Social Networking Sites'.

Personal devices and bring your own device (BOYD) procedures:

We recognise the widespread use of personal devices makes it essential that academies take steps to ensure mobile phones and devices, including wearable or "smart" technologies like health or fitness trackers, are used responsibly whilst in school and it is essential that student use of their devices does not impede teaching, learning and good order in classrooms. Staff will be given clear boundaries on professional use.

Mobile devices can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;

- Their use can render student or staff subject to cyberbullying;

- Apps or mobile devices which broadcast location data can make staff or students vulnerable to behaviours like stalking and can provide perpetrators with information to take cyberbullying into the real world;

- Internet access on phones and personal devices can allow students to bypass security settings and filtering;

- They can undermine classroom discipline as they can be used on "silent" mode;

- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues in relation to inappropriate capture, use or distribution of images of students or staff;

Permitted use of mobile phones and personal devices is an academy decision and the following will apply:

- The use of mobile phones and other personal devices by students and staff whilst in the academy will be decided by the Trust and covered in the Acceptable Use Agreement.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Trust community and any breaches will be dealt with as part of the Trust's/academies discipline/Behaviour policies.

- The academies reserve the right to search the content of any mobile or handheld devices on academy premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence, or bullying.

- Trust staff may confiscate a phone or device if they believe it is being used to contravene the academy's Behaviour policy or bullying procedures.

- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. They should be switched off (not placed on silent) and stored out of sight on arrival at school. Staff members may use their phones during break times. All visitors are requested to keep their phones on silent whilst in the academy.

- The recording, taking, and sharing of images, video and audio on any mobile phone is not permitted.

- The Bluetooth function of a mobile phone should always be switched off and not be used to send images or files to other mobile phones.

- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft, or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break time.

- Mobile phones and personal devices are not permitted to be used in certain areas within the academy sites such as changing rooms and toilets.

Students' use of personal devices:

- The Trust strongly advises that student mobile phones should not be brought into the academy. However, the academy accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, the circumstances should be discussed with the class teacher and the normal rules regarding use during the academy day will apply.

- If a student breaches the academy's procedures, then the phone or device will be confiscated and will be held in a secure place in the Head of Year's office. Mobile phones and devices will be released to parents in accordance with the academy's procedures.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- If a student needs to contact their parent, they will be allowed to use an academy phone. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office.

- Students should protect their phone numbers by only giving them to trusted friends and family members.

- Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff use of personal devices:

•   Staff are not permitted to use their own personal phones or devices for contacting children, young people, and their families within or outside of the setting in a professional capacity.

•   Staff will be issued with an academy phone where contact with students or parents is required.

•   Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off, location data switched off unless being used only for the duration of a specific task like route directions on a school trip, and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of the leadership team for emergency circumstances.

•   If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the leadership team.

•   Staff must not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.

•   Where members of staff are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then an academy mobile phone will be provided and used. In an emergency where a staff member does not have access to an academy-owned device, they should use their own device and hide their own mobile number for confidentiality purposes.

•   If a member of staff breaches the Trust's policy and procedures, then disciplinary action may be taken.

Parents are asked to keep phones out of sights whilst on academy premises. They must ask permission before taking any photos e.g., of displays in corridors or classrooms and avoid capturing other children. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the academy office.

Network/internet access on school devices

Students are not allowed networked file access via personal devices. However, they are permitted to access the academy wireless internet network for academy-related internet use/limited personal use within the framework of the Acceptable Use Agreement. All such use is monitored.

Searching, Screening and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Principal and staff authorised by them have a statutory power to search students/property on Trust premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, upskirting, violence or bullying. Further details are available in the Whole School Behaviour policy and procedures.

10.   MANAGING FILTERING AND MONITORING

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn we (the Governors, SLT and staff) will do all we reasonably can to limit children's exposure to online safety risks from the school's IT system. As part of this process, we will ensure that the school has appropriate filtering and monitoring system in place and will regularly review their effectiveness.

By making use of an appropriate risk assessment, the school will work towards meeting the obligations set out in the DfE filtering and monitoring standards which set out that schools should:
•   identify and assign roles and responsibilities to manage filtering and monitoring systems.
•   review filtering and monitoring provision at least annually.
•   block harmful and inappropriate content without unreasonably impacting teaching and learning.
•   have effective monitoring strategies in place that meet their safeguarding needs

The Governors will review the standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting the standards.
The following issues will be addressed in relation to the management of filtering:

•   The academy's broadband access will include filtering appropriate to the age and maturity of students.

•   The academy will work with the Trust's Broadband team, Virtue, to ensure that filtering procedures are continually reviewed.

•   The academy will have a clear procedure for monitoring and subsequent reporting breaches of filtering. All members of the academy community (all staff and all students) will be aware of this procedure.

•   If staff or students discover unsuitable sites, the URL will be reported to the academy's Online Safety Coordinator/DSL who will then record the incident and escalate the concern as appropriate.

•   The academy's filtering system will block all sites on the Internet Watch Foundation (IWF) list.

•   Changes to the academy's filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the leadership team.

•   The academy leadership team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

•   Any material that the academy believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP.

•   The Trust's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from the Network Manager.

Filtering on school networks must not be tested by searching for content that is known to be filtered because it is harmful. South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school's filtering provider is signed up to relevant lists (CSA

content, Sexual Content, Terrorist content Your Internet Connection Blocks Child Abuse & Terrorist Content).

11. WEBCAMS AND SURVEILLANCE CAMERA SYSTEMS (incl.CCTV)

The school uses a surveillance camera system for security and safety. The only people with access to the surveillance camera system is/are (state who). Notification of camera system use is displayed at the front of the school and at various points throughout the building so that individuals are aware that a surveillance camera system is in operation. Staff will refer to the Information Commissioners Office (ICO) for further guidance and the school surveillance camera system procedures.

In relation to webcams:

- We do not use public (unrestricted) access webcams in school unless we are livestreaming an appropriate educational project such as construction work or egg-hatching in a way that does not capture images of children or adults and positioning is checked regularly e.g., disabling any microphone, and siting the camera so only the eggs are visible, or so far away from construction work that people are not identifiable.

- We only use private (restricted) access webcams with children or adults when it is necessary e.g., for educational purposes or school management reasons (commonly remote education, Teams meetings between colleagues and other professionals, and live online training platforms) and when we have conducted a DPIA which indicates it is reasonable to and that recordings or streaming will be appropriately secure.

- All webcams that are not in use are covered and access to the device's microphones is disabled so that if accessed in an unauthorised way, it will not function to broadcast anything usable.

- Misuse of the webcam by any member of the academy community will result in sanctions.

- As for all images, content captured by webcams can only be published if student and parental consent is valid.

12. MANAGING EMERGING TECHNOLOGIES

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration, and multimedia tools. We will undertake a risk assessment on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safe practice has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the Trust may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype, and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication but is often not possible. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster internet access, enable video to be exchanged across the Internet. The availability of live video can

sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details. New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless internet access. This can offer immense opportunities for learning as well as dangers such as a student using a phone to video a teacher's reaction in a difficult situation.

The Trust should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance, whether communicating with a pupil or families via SMS or an instant messaging app about a pupil's absence or to send reminders for [insert suitable example e.g., exam coursework] is appropriate in some or all cases. There are dangers for staff if personal devices or accounts are used to contact pupils so, we will endeavour to make a school owned device or account available if this kind of contact is necessary.

The inclusion of inappropriate language or images is difficult for staff to detect. Students may need reminding that such use is inappropriate and conflicts with Trust policy and procedures. Abusive messages should be dealt with under the Whole School Behaviour Policy.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in an academy is allowed.

- Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Acceptable Use Agreement.

13.   CYBER SECURITY AND RESILIENCE

It is vital that the school understand our vulnerabilities in relation to potential cyber-attacks and breaches, regularly review our existing defences and take the necessary steps to protect our networks. As well as having a current and cohesive Cyber Response Plan in place, there are several measures that we can implement to help to improve our IT security and mitigate the risk of a cyber-attack. These measures fall under the 'Identify, Protect and Detect' pillars of effective cyber resilience and are outlined in our cyber security and resilience strategy. A copy of our strategy is available on request from the school office.

14.   POLICY DECISIONS

14.1   Authorising internet access

The Trust will allocate internet access to staff and students based on educational need. It will be clear who has internet access and who has not. Normally most students will be granted internet access. We will not prevent students from accessing the Internet unless the parents have specifically denied permission, or the child is subject to a sanction as part of the Whole School Behaviour policy.

- The academy will maintain a current record of all staff and students who are granted access to the academy's electronic communications.

- All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources.

- Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.

- Parents will be informed that students will be provided with supervised internet access appropriate to their age and ability.

- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to setting type:

- At key stage 1 students' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

- At key stage 2 students will be supervised. Students will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

- Secondary students will apply for internet access individually by agreeing to comply with the school online safety rules and Acceptable Use Agreement

14.2 Assessing risks

As the quantity and breadth of information available through the internet continues to grow it is not possible to guard against every undesirable situation. The Trust will need to address the fact that it is not possible to completely remove the risk that students might access unsuitable materials via the Trust system.
Risks can be considerably greater where tools are used which are beyond theTrust's control such as most popular social media sites.

- The Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via an academy computer. The Trust cannot accept liability for the material accessed, or any consequences resulting from internet use.

- The Trust will audit ICT use to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see Appendix A for a sample Online Safety Audit.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police using 101 or the appropriate online report from available from our local Constabulary website.

- Methods to identify, assess and minimise risks will be reviewed regularly.

14.3 Responding to incidents of concern

Refer to Section 3 above.

15. COMMUNICATING POLICY AND PROCEDURES

15.1 Introducing the policy and procedures to Students

Many students are very familiar with the culture of mobile and internet use, so we try to involve them in the development of the Trust's Online Safety Policy, through "student voice" activities like the School Council. As students' perceptions of the risks will vary, the online safety rules will be explained or discussed in an age-appropriate manner.

Online safety student and parental engagement programmes we can use include:

• Think U Know: www.thinkuknow.co.uk
• Childnet: http://www.childnet.com

Student induction and ongoing training and education will include:

• Informing all users that network and internet use will be monitored.

• Establishing an online safety training programme across the Trust to raise the awareness and highlight the importance of safe and responsible internet use.

• Student instruction regarding responsible and safe use before internet access is given.

• An online safety module in the PSHE, Citizenship and/or ICT programmes covering both safe academy and home use.

• Online safety training as part of the transition programme across the key stages and when moving between academies or other educational or training settings.
• Accessible Online Safety rules or copies of the student Acceptable Use Agreement including posters in all rooms with computers/internet access.

• Regular reinforcement of safe and responsible use of the Internet and technology across the curriculum, in all subject areas, and extended schools or extra- curricular activities.

• Particular attention paid to Online Safety education where students are considered to be vulnerable.

15.2   Discussing the policy and procedures with Staff

It is important that all staff feel confident meeting the demands of using ICT appropriately in teaching, administration, and all other aspects of their academy and personal life and the Trust Online Safety policy and procedures will only be effective if all staff subscribe to its values and methods.

Staff will be given opportunities to discuss the issues and develop appropriate teaching or other work strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an internet activity without preparation.

Any member of staff who has concerns about any aspect of their own or anyone else's ICT or internet use either on or off site, they should discuss this with their line manager. Where concerns are related to children's safeguarding, they should also be reported to the DSL who should follow the Child Protection policy and procedure for recording and reporting allegations that meet the harm threshold and recording (and in some case reporting i.e., to a contractor's employer) low level concerns that do not.

Consideration is given when members of staff are provided with devices by the Trust which may be accessed outside of the Trust network. Staff are made aware of their responsibility to maintain the security and confidentiality of school information.

All staff have a universal duty to understand harms and protect children from them, including online. ICT use is widespread and all staff including administration, midday supervisors, facilities staff, trustees, governors and volunteers who use it or work with children who use it are included in awareness raising and training.

Induction of all new staff will include:

• A copy of the Online Safety policy and procedures and a scheduled opportunity to discuss them.

• That internet traffic can be monitored and traced to the individual user, and the importance of having high professional standards and always following current policies and procedures.

• Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally.

• Requirement to read, understand and sign relevant Acceptable Use Agreements.

• For staff who manage filtering systems or monitor ICT use: that they will be supervised by the Senior Leadership Team and what the procedures for reporting issues are.
• How the Trust will promote online tools which staff should use for work purposes, especially with children, and the procedure staff should go through if there is a new tool they want to use.

• That their online conduct out of the trust could have an impact on their role and reputation in the Trust. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Volunteers will receive an online safety induction based on what staff receive but suitable for the role they have been asked to fulfil.

When we employ an Early Career Teacher (ECT replacing newly qualified teacher or NQT) or work with trainee teachers the OSL will ensure use of the UKCIS Online Safety Audit Tool or similar self-assessment with them to help them better understand their role in keeping children safe online and our policy and practice.

15.3   Enlisting Parents' Support

Internet use in students' homes is increasingly widespread. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The academy may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

To engage with parents and carers we will:

• draw attention to our Online Safety policy and procedures in newsletters, and on the academy website;

• encourage a partnership approach to online safety at home and at school which may include demonstration evenings, regular suggestions for safe home internet use, promoting educational online safety activities for families, or highlighting online safety issues at other attended events e.g., parent evenings and sports days;

- ask parents and carers to read and sign the school Acceptable Use Agreement for younger students and discuss its implications with their children and offer support to do this if required;

- provide information and guidance for families about on online safety in a variety of formats;

- provide advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet;

- refer interested parents to organisations listed in the "online safety Links" at Appendix K;

- advise that they check whether their child's use of the Internet elsewhere in the community is covered by an appropriate Acceptable Use Agreement and if they understand the rules.

16.   COMPLAINTS

The Trust will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable materials will never appear on an academy computer or mobile device. Neither the Trust staff nor the Trust and governing boards can accept liability for material accessed, or any consequences of internet access.

- Complaints about the misuse of on-line systems will be dealt with under the Trust's Complaints procedure.

- Complaints about cyberbullying are dealt with in accordance with academy Anti-bullying procedures which form part of the Whole School Behaviour policy and procedures.

- Complaints related to child protection are dealt with in accordance with the academy's Child Protection Policy and procedures.

- Any complaints about staff misuse will be referred to the Principal.

- All online safety complaints and incidents will be recorded by the academy including any actions taken (see Appendix H).

Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling   by   class   teacher/Head   of   Year/Online   Safety Coordinator/Principal;
- informing parents;
- removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework);
- referral to the Police.

ONLINE SAFETY LINKS

This list provides links to relevant government guidance and a range of national organisations who can offer support to schools.

Related guidance is available on:

- [relationships and sex education (RSE) and health education](#)
- [national curriculum in England computing programmes of study](#)
- [national curriculum in England citizenship programmes of study](#)

Support and resources are also available from:

- [National Centre for Computing Education (NCCE)](#)
- [UK Council for Internet Safety](#)
- [UK Safer Internet Centre](#) (UKSIC)
- [Education for a Connected World](#)
- [CEOP](#) (Child Exploitation and Online Protection Centre)
- [CEOP Education Programme](#) (Thinkuknow.co.uk)
- [Cumbria Safeguarding Children Partnership](#) (Cumbria SCP)
- [Information Commissioner's Office (ICO)](#)
- [Teaching online safety in schools](#)
- [The PREVENT Duty – DfE non-statutory Departmental advice for Schools and Childcare Providers](#)
- [How social media is used to encourage travel to Syria and Iraq: briefing note for schools](#) – Home Office advice
- [Internet Watch Foundation (IWF)](#)
- [Smoothwall](#)

Schools can also get advice from national organisations such as:

- [Anti-Bullying Alliance](#)
- [Association for Citizenship Teaching](#)
- [The Diana Award](#)
- [DotCom Charity](#)
- [Hopes and Streams](#)
- [Internet Matters](#)
- [NSPCC learning](#)
- [Parent Zone's school resources](#)
- [PSHE Association](#)
- [SWGfL](#)
- [Better Internet for Kids](#)
- [Virtual Global Taskforce — Report Abuse](#)
- [Cyberbullying.org](#)

You can refer parents to the following national organisations for support:

- [Internet Matters](#)
- [NSPCC](#)
- [Parent Zone](#)
- [Facebook Advice to Parents](#)
- [Family Online Safety Institute](#) (FOSI)
- [Get safe online - Test your online safety skills](#)

You can refer pupils to the following national organisations for support:

- [BBC Own It](#)

- [Childline](#)
- [Childnet](#)

Appendix A

CHANGING LIVES LEARNING TRUST STUDENT ICT ACCEPTABLE USE AGREEMENT

- I will only use Information and Communication Technologies (ICT) systems in the academy, including the internet, email, digital video, mobile technologies, etc. for educational purposes.

- I will only log on to the academy network/Learning Platform, other systems and resources with my own username and password. I will not share my username and password, nor will I try to use any other person's username or password.

- I will follow the academy's ICT security system and not reveal my passwords to anyone and change them regularly.

- I will only use my academy email address for educational purposes. I will check my email regularly and carry out routine "housekeeping" of my email messages.

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

- I will not arrange to meet anyone I have met over the internet.

- I will make sure that all ICT communications with students, teachers or others is responsible, polite, and sensible. I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.

- I will 'log off' when leaving a computer.

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

- I will only save files to the network that are related to schoolwork. I will not use filenames that could be considered offensive.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

- I will not take photographs, video or audio of staff nor other students in the trust without their permission.

- I am aware that when I take images of students and/or staff, that I must only store and use these for school purposes and in line with school procedures and must never distribute these outside the school network without the permission of all parties involved, including in school breaks and all occasions when you are in academy uniform or when otherwise representing the academy.

- I will not bring in discs and USB pens or other portable devices from home without permission. I will screen all such devices for malicious software before I connect or load any files onto the Trust network.

- I will not attach any device to the Trust network which may contain files which breach copyright, data protection or other laws.

- I agree not to bring in ICT hardware from outside of the Trust and use this hardware on the Trust network.

- I will ensure that my online activity, both in the academy and outside the academy, will not cause my academy, the staff, students, or others distress or bring the academy community into disrepute, including through uploads of images, video, sounds or texts.

- I understand that I am responsible for my actions, both in and out of the academy and that the academy has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am out of the academy and where they involve my membership of the academy community (e.g., cyberbullying, use of images or personal information etc.)

- I understand that the academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- When I am using the Internet to find information, I should take care to check that the information that I access is accurate as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

- I will always respect the privacy and ownership of others' work online and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission. Where work is protected by copyright, I will not try to download copies (including music and videos).

- I will avoid plagiarism by not passing off work downloaded from the internet as my own.
- I will give clear references to sources were I have downloaded someone else's work.

- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will only use my personal hand-held/external devices in the academy if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment.

- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

- I will not open any attachments to emails unless I know and trust the person or organisation that sent the email due to the risk of the attachment containing a virus or other harmful programme.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

- I will only print copies of my work when it is really necessary. I will reduce my printing by selecting page or printing handouts. I will only print in colour when this is essential to my learning. I understand that the Trust will monitor any printing that id o and may take action if this is excessive.

- I will notify an adult immediately if I suspect someone of misusing ICT facilities, social media or the internet.

- I will ensure my personal portable device allocated to me is brought to the academy ready for use.

- I understand I am responsible for the use and care of any portable device intended for my personal use whilst a student at the academy.

- I will respect Trust resources and not damage or steal ICT facilities.

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

- I understand that these rules are designed to keep me safe and that if they are not followed, academy sanctions will be applied, and my parent may be contacted, and any illegal activities will be reported to the Police.

Student ICT Acceptable Use – Student <u>and</u> Parent Agreement

Dear Parent

ICT including the Internet, learning platforms, email and mobile technologies and online resources have become an important part of learning in our academy. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of online safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign this declaration and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher or Head of Year. A parent or carer is also asked to sign below to acknowledge that this agreement is in place.

I have read and understood the above statements and I agree to comply with the Trust rules for the use of ICT facilities, social media and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Name of Student:		Class/Year Group:	
Student Signature		Date:	

As the parent or legal guardian of the student signing above, I grant permission for them to use electronic mail, social media and the internet. I understand that students will be held accountable for their own actions. I also understand that some material on the internet or social networking sites may be objectionable and I accept responsibility for setting standards for them to follow when accessing selecting, sharing and exploring information and media.

Name of Parent/Carer:			
Parent Signature		Date:	

Thank you for your continued support

Appendix B

STAFF / VOLUNTEER ICT ACCEPTABLE USE AGREEMENT

The use of Information and Communication technologies (ICT and personal data) such as email, the Internet, and mobile devices are an expected part of daily working life in school. This Agreement is designed to ensure that all staff and volunteers are aware of their responsibilities when using any form of ICT. It applies to any ICT used in school, the use of school ICT systems and equipment out of school and the use of personal equipment in school or in situations related to their employment by the school. All staff and volunteers (where they are using technology in school or in connection with the work of school) are expected to sign this Agreement and always adhere to its content. Any concerns or clarification should be discussed with your Online Safety Lead Principal.

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal, and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that the children or young people in their care are safe users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

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

- I will only use my own usernames and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis [90 days]

- I will not use any other person's username and password.

- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students.

- I will not use any personal social media accounts for Trust business.

- I will not use WhatsApp for official Trust business.

- I will register with the Network Support Team and Trust PR Manager any new social media accounts specifically created for Trust business.

- I will ensure that all personal data which I have access to is kept secure in compliance with UK GDPR, trust systems, policies and procedures.

- I will report any loss or breach of personal data immediately to the Trust's Data Protection Officer.

Appendix B

- I will not attach any device to the network which may contain files which breach copyright, data protection and other laws.

- I agree to use the Trust's ICT facilities, social media and internet only for work related use during my working hours.

- I will not search, view, send or display offensive materials such as pornography.

- I will not use the Trust's ICT facilities for personal financial gain, gambling, political purposes, advertising or cause damage to the trust's reputation. I will only access social networking sites to enhance the teaching and learning experience for students.

- I will not send offensive, threatening or time-wasting message not post inappropriate images on websites. All email sent will be of a professional nature and appropriate to its audience.

- I will only print copies of my work when it is really necessary. I will reduce my printing by selecting pages or printing handouts.

- I will ensure that my data is regularly backed up.

- I will ensure that I 'log off' after my network session has finished.

- If I find an unattended machine logged on under another user's username, I will not
- continue using the machine – I will 'log off' immediately.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the Trust into disrepute.

- I will not accept invitations from Trust students to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

- As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities as a Governor at the school, such as parents and their children.

- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.

- I will only transport, hold, disclose or share personal information about myself or others as outlined in the Trust's personal data guidelines.

- Where personal data is transferred outside the secure trust network, it must be encrypted. Personal data can only be taken out of the academy when authorised, in advance, by the DPO/Principal. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g., on a password secured laptop or memory stick. Staff

leading a trip are expected to take relevant student information with them, but this must always be held securely.

- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:

- do not reveal confidential information about the way the academy operates;
- are not confused with my academy responsibilities in any way;
- do not include inappropriate or defamatory comments about individuals connected with the academy community;
- support the academy's approach to online safety which includes not uploading or posting to the Internet any pictures, video or text that could upset, offend, or threaten the safety of any member of the academy community or bring the academy into disrepute;

- I will not try to bypass the filtering and security systems in place.

- I will only use my personal ICT in the academy for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses by having these checked by the Network Support team.

Promoting Safe Use by Learners

- I will support and promote the Trust's Online Safety, Data Protection and Behaviour Policies and help students to be safe and responsible in their use of ICT and related technologies.

- I will model safe use of the internet in the trust.

- I will educate young people on how to use technologies safely according to the academy teaching programme.

- I will take immediate action in line with academy procedures if an issue arises in the academy that might compromise a learner, user, or academy safety or if a student reports any concerns.

- I will only use the academy's email/Internet/learning platforms and any related technologies for professional purposes or for uses deemed 'acceptable' by the Principal or governing board.

- I will communicate on-line in a professional manner and tone; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

- I will not use language that could be calculated to incite hatred against any ethnic, religious, or other minority group.

- I will only communicate with students and parents using the Trust's approved, secure email system. Any such communication will be professional in tone and manner.

- I am aware that any communication could be forwarded to an employer, trustee or governor.

- I will only use chat and social networking sites that are approved by the academy.

- I will not use personal email addresses on the academy ICT systems unless I have permission to do so.

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory, or inappropriate or may cause harm or distress to others.

- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.

- I know that all Trust ICT is primarily intended for educational use, and I will only use the systems for personal or recreational use if this is allowed by the academy.

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.

- I will always respect the privacy and ownership of others' work online and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.

- Images of students and/or staff will only be taken, stored, and used for professional purposes using academy equipment in line with academy procedures.

- I will only take images/video of students and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.

- If images are to be published online or in the media, I will ensure that parental/staff permission allows this.

- I will not use my personal equipment to record images/video unless I have permission to do so from the Principal or other Senior Manager.

- I will not keep images and/or videos of students stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.

- Where these images are published (e.g., on the academy website/prospectus), I will ensure that it is not possible to identify the people who are featured by name or other personal information.

- I will support the academy's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the academy community.

Buying/Selling/Gaming

I will not use academy equipment for on-line purchasing, selling, or gaming unless I have permission to do so.

Problems

- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, to the Online Safety Coordinator or Principal.

- I will not install any hardware or software on a computer or other device without permission of the Network Manager.

- I will not try to alter computer settings without the permission of the Network Manager.

- I will not cause damage to ICT equipment in the academy.

- I will ensure that I follow relevant health and safety legislation when using ICT facilities such as not looking into the light beam from a projector and not leaving students unsupervised around projectors/interactive white boards.

- I will ensure that ICT facilities are left in a fit state for the next person or class to use them.

- I will immediately report any damage or faults involving equipment or software; however this may have happened.

- I will ensure that any personal device allocated to me is brought to the academy ready for use.

- I understand that I am responsible for the safe keeping of any ICT equipment which I use, including such equipment which I may take off site. I will not remove ICT equipment from the site without signing it out from the Network Support team.

- I understand that I must adhere to all relevant policies and procedures including, but not limited to, Staff Code of Conduct, Child Protection and professional standards. As examples the following are not permitted: sharing of personal messages, photographs, video and audio, language must always be professional and appropriate; use of emoji is not views as appropriate. This list is not exhaustive.

- I will not allow students to use my trust tablet/iPad/mobile phone.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I understand this forms part of the terms and conditions set out in my contract of employment.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to trustees, governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Staff/Volunteer ICT Acceptable Use Agreement

I will use the trust network in a responsible way and observe all the restrictions as explained in the staff ICT Acceptable Use Agreement. I agree to use ICT by these rules when:

✓ I use school ICT systems at school, at home, or in other public or private spaces when I have permission to.
✓ I use my own ICT (where permitted) in school.
✓ I use my own ICT out of school to access school sites or for activities relating to my work or volunteering for school.

Staff/Volunteer Name:			
Job Title (if applicable):			
Signature:		Date:	

Thank you for your continued support

Changing Lives Learning Trust

MEMBER/TRUSTEE/GOVERNOR ICT ACCEPTABLE USE AGREEMENT

The use of Information and Communication technologies (ICT - and personal data) such as email, the Internet, and mobile devices may all be an expected part of trust governance. This Agreement is designed to ensure that all Members, trustees and governor are aware of their responsibilities when using any form of ICT as it relates to their role in the trust. It applies to any ICT used in the trust, to the use of trust ICT systems and equipment out of trust and the use of personal equipment in individual academies or in situations related to MAT governance. All Members, trustees and governors (where they are using technology in relation to their role) are expected to sign this Agreement and always adhere to its contents.

This Acceptable Use Agreement is intended to ensure that:

• Members, trustees and governors are responsible users and stay safe while using technologies for educational, personal, and recreational use;

• Trust ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;

• Members, trustees and governors are protected from potential risk from the use of ICT.

If you make a comment about the trust or its academies you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the trust or its academies into disrepute is not permitted.

All users are required to follow the conditions laid down in the Agreement. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of the services, and in some instances could lead to criminal prosecution.

Personal Responsibility

Users are responsible for their behaviour and communications.

• Members, trustees and governors are expected to use the resources for the purposes for which they are made available.

• It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Agreement, and to ensure that unacceptable use does not occur.

• Users will accept personal responsibility for reporting any misuse of the network to the Principal/Chair of Trustees/Governors.

Keeping Safe

• I will not reveal any personal information (e.g., home address, telephone number, social networking details) of other users to any unauthorised person.

• I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students.

- I will only use my own usernames and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis and always where I think someone may have learned my password.

- I will not use any other person's username and password or, where they are known, pass the details to any other individual.

- I will not attempt to access other users' files or folders.

- I will ensure that I 'log off' after my network session has finished.

- If I find an unattended machine logged on under another user's username, I will not
- continue using the machine – I will 'log off' immediately.

- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

- I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Principal as soon as I become aware of the access/receipt.

- I will not accept invitations from students to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.

As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities as a Member, trustee, governor at the trust, such as parents and their children.

- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:

  - Do not reveal confidential information about the way the trust operates.
  - Are not confused with my trust responsibilities in any way.

Promoting Safe Use by Learners

- I will support and promote the Trust's Online Safety and Data Security policies and procedures and help students be safe and responsible in their use of the Internet and related technologies.

Communication

- I will not create, transmit, display, or publish any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person or bring the trust and its academies into disrepute.

- I will use appropriate language – I will remember that I am a representative of the trust on a global public system. Illegal activities of any kind are strictly forbidden.

- I will not use language that could be calculated to incite hatred against any ethnic, religious or minority group.

I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the Principal. Anonymous messages are not permitted.

I will not send or publish material that violates the Data Protection Act or breaches the security this Act requires for personal data.

I will not receive, send, or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.

I will ensure that any personal data (where the Data Protection Act applies) that is sent over the Internet (or taken off-site in any other way) will be encrypted.

Sharing

☐ I will not use personal digital cameras or camera phones for creating or transferring images of children or young people without the express permission of the academy's leadership team.

General Equipment Use

- I will not use the network in any way that would disrupt the use of the network by others.

- I will not use tablets or personal laptops on the network without having them 'approved' by the trust and checked for viruses.

- I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.

- I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

- I understand that I must comply with the Acceptable Use Agreement of any other network which is accessed via the school network.

Users of the trust network are expected to inform the Principal/Chief Operating Officer/Chief Finance Officer immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the academies' networks will be regularly checked and monitored. Users identified as a security risk will be denied access to the network.

Changing Lives Learning Trust Member, Trustee and Governor Acceptable Use Agreement

As a user of the network resources, I agree to follow the trust rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the trust's Online Safety Policy and procedures and Acceptable Use Agreement. If I am in any doubt, I will consult the Principal.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that Members, trustees and governors under reasonable suspicion of misuse in terms of access or content may be placed under retrospective investigation or have their usage monitored.

Name:			
Signed		Date:	

Thank you for your continued support