E-SAFETY POLICY

Approved and signed by the Board of Trustees

26.09.22

Next Review: Feb 2024

CONTENTS

APPENDICES

CHANGES

May 2017
Policy adopted by the Board of Trustees. This policy has been adapted from the South West Grid for Learning Online Safety Policy, with appropriate amendments made for the purposes of Discovery Multi Academy Trust's arrangements.

Jun 2020
Policy updated with appropriate minor amendments.

Sept 2021
Policy updated with appropriate minor amendments.

Sept 2022
Policy updated with appropriate minor amendments.

1 SCHEDULE FOR REVIEW & MONITORING

This E-Safety policy was approved by the Board of Trustees on	26.09.22
The implementation of this E-Safety policy will be monitored by the:	Alison Nettleship – CEO/ Executive Headteacher
Monitoring will take place at regular intervals:	Annually
The Board will receive a report on the implementation of the E-Safety policy (which will include anonymous details of E-Safety incidents) at regular intervals:	September each year
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be:	2023
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	Plymouth Children's Safeguarding Board – Plymouth City Council, Police

The MAT will monitor the impact of the policy using:

- logs of reported incidents;
- monitoring logs of internet activity (including sites visited);
- internal monitoring data for network activity; and
- surveys / questionnaires of pupils, parents, carers and staff.

2 SCOPE OF THE POLICY

This policy applies to all members of the Discovery Multi Academy Trust ("the MAT") community, (including staff, pupils, volunteers, parents, carers, visitors and those in a position of governance) who have access to and are users of MAT ICT systems, both in and out of the MAT.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered in the MAT's Managing and supporting positive behaviour policy.

The MAT's academies will deal with such incidents as outlined by the detail given within this policy, as well as the MAT's Managing and supporting positive behaviour policy and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school hours.

3 ROLES AND RESPONSIBILITIES

The following section outlines the E-Safety roles and responsibilities of individuals and groups within Discovery Multi Academy Trust:

- Chief Executive Officer (CEO)/Executive Headteacher/Designated Lead for Safeguarding - Alison Nettleship
- Heads of School/Deputy Designated Leads for Safeguarding – Mrs Tamsin Bailey (Beechwood), Jackie Sparrow (Oakwood), Kathryn Catherwood (Weston Mill)
- Facilities & ICT Manager – Mr Leslie Rust
- ICT External Support – Eggbuckland Community College
- E-safety Co-ordinator – As designated by Head of School/or Computing Co-ordinators.

3.1 The Board of Trustees

The Board are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about E-Safety incidents and monitoring reports. The Chair of the Board, as part of their role as Safeguarding Trustee (see **Safeguarding Policy**), will carry out the following:

- Regular monitoring of E-Safety incident logs (through Behaviour Watch)
- Regular monitoring of filtering / change control logs
- Reporting to the Board

3.2 Chief Executive Officer (CEO) and Senior Leaders

- The CEO has a duty of care for ensuring the safety (including E-Safety) of members of the MAT community, though the day to day responsibility for E-Safety will be delegated to the Computing/E-safety Co-ordinator and Head of School.
- The CEO and Head of School should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- The CEO is responsible for ensuring that the Head of Schools and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The CEO will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing/E-Safety Co-ordinator / Officer.

3.3 ICT Manager

The ICT Manager is responsible for ensuring:

- that the MAT's technical infrastructure is secure and is not open to misuse or malicious attack
- that the MAT meets required E-Safety technical requirements and any Department for Education (DfE) Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network / internet / virtual learning environment / email is regularly monitored in order that any misuse / attempted misuse can be reported to the CEO and Head of School for investigation.
- that monitoring software and systems are implemented and updated as agreed in MAT policies.
- takes day to day responsibility for E-Safety issues and has a leading role in establishing the school E-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- receives reports of E-Safety incidents and creates a log of incidents to inform future ESafety developments
- meets regularly with E-Safety Trustee to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings
- reports regularly to Senior Leadership Team

3.5 Teaching and Support staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current MAT E-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy **(Appendix A)**
- they report any suspected misuse or problem to the CEO and Head of School for investigation using Behaviour watch.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety policy

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- E-safety incidents are followed up with literature from the National Online Safety Platform so that children/parents have correct and up-to-date information about technology, applications and other online software.

3.6 Designated Lead for Safeguarding

The Designated Lead for Safeguarding should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- prolonged exposure to online technologies, particularly from an early age
- exposure to illegal, inappropriate or harmful content
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyberbullying
- making, taking and distribution of illegal images and "sexting"
- physical, sexual and emotional abuse
- identity theft
- privacy issues
- addiction to gaming or gambling
- pressure from the media and targeted advertising
- theft and fraud from activities such as phishing
- viruses, malware, etc
- damage to professional online reputation through personal online behaviour.

3.7 Pupils

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

3.8 Parents / Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The MAT will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns / literature. Each school also has a unique E-safety Platform provided by the 'National Online Safety Platform' where they can become part of our school community and be able to access a plethora of E-safety training and resources.

Parents and carers will be encouraged to support the MAT in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

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

3.9 Community Users

Community users (volunteers, supply teachers) who access MAT systems / website / VLE as part of the wider MAT provision will be expected to sign a Community User Acceptable Use Agreement **(Appendix C)** before being provided with access to school systems.

4 POLICY STATEMENTS

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the MAT's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. The Keeping Children Safe in Education (2021) document acknowledges that whilst technology is an important vehicle within today's society it is also 'a significant component in many safeguarding and well-being issues.' Children are at risk of many forms of abuse including (but not limited to): peer on peer abuse, emotional abuse and physical abuse as well as forms of exploitation. Discovery MAT aims to provide a safe environment for all children to learn about acceptable and unacceptable uses of technology and share concerns of any technology use that they feel is affecting their well-being.

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

- A planned E-Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Where pupils access content provided by the Trust via eSchools or any other platform are not allowed to share on any type of social media or copy to any other device or platform, but only to be used for what it intended for.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Computing and E-safety Curriculum Statements:

Beechwood Primary Academy – Computing

As the trust continues to develop its resources and expertise to deliver the Computing and E-safety curriculum; units are planned in line with the national curriculum objectives and follow skills and knowledge identified on the Computing/E-safety Progression Map(s). Each year, the children will experience different units that build on skills and knowledge taught in previous years to ensure that all children are given the ability to thrive and engage with the Computing curriculum.

Units are designed to enable pupils to achieve stated objectives through a broad and balanced curriculum that develops skills and knowledge in a cross-curriculum fashion. Not only do children have access to a wide range of equipment but our Progression Map has been developed to focus on using innovative and creative teaching strategies in an 'unplugged' fashion to support children learning the required knowledge, before tinkering with equipment and applying their knowledge through the practising of skills. The E-safety Progression Map has been is reviewed annually and is based on individual units shared by National Online Safety Platform linked with the UK Council for Internet Safety's 'Education for a Connected World' 2020 framework. All children experience a broad and balanced curriculum where the end of units are shared through destinations showcasing the learning journey of a class or year group encapsulating a STEM focus. Often, children use ICT to share their learning and bring together termly cross-curricular units. Children also have access to 'Renaissance Reading' an website that provides a range of resources to support raising attainment with Reading.

Staff link units together using a long-term plan driven through Science. Staff then plan using the progression map and the National Curriculum objectives. Units are planned using daily planning sheets; where all subjects are linked in a cross-curricular fashion to ensure robust coverage. Children who need additional support are identified and supported during lessons. Teachers assess attainment regularly using assessment for learning strategies in class and using our online assessment platform. This allows for Teachers to assess necessary gaps and planned to demise these in future lessons.

Our children are also encouraged to take part in richer Computing experiences such as Hour of Code, and are encouraged through trips to make links with local schools; colleges, businesses and universities. Children also have ICT opportunities to communicate safely with other children across the world through our Connecting Classrooms International Learning Project.

Oakwood Primary Academy - Computing

Computing and E-safety units are planned in line with the national curriculum objectives and follow skills and knowledge identified on the computing progression map. Teachers also use an E-safety Progression Map that is reviewed annually and is based on individual units shared by National Online Safety Platform linked with the UK Council for Internet Safety's 'Education for a Connected World' 2020 framework to deliver E-safety units termly to all children in all year groups. Children in every year group will have the opportunity to experience a variety of units which build on previously taught skills and knowledge, ensuring that all children are given the ability to engage and succeed with the Computing Curriculum.

Units are designed specifically to enable pupils to achieve stated objectives within a broad and balanced curriculum, that develops skills and knowledge in a cross-curricular manner. Children will have access to a range of equipment such as ipads, chrome books and robots for hands on practise. Additionally, they will be exposed to innovative and creative teaching strategies in an 'unplugged' fashion to pre-teach the required terminology and skills before developing these through practising with technology. All children experience a broad and balanced curriculum and have the opportunity to showcase their learning through a range of mediums at the end of units. Often, children may use ICT to share in a cross-curricular way during different lessons to present work or display outcomes. The online programme Renaissance Reading is used widely in school to engage children with their reading and celebrate success by allowing them to complete quizzes and gain certificates. It also allows adults to easily assess progress and to target gaps in their classes reading and comprehension skills by generating a wide variety of reading data.

Staff link together units using a long term plan driven through STEM. Staff then plan using the progression map and the National Curriculum objectives. Units are planned using daily planning sheets; where all subjects are linked in a cross-curricular fashion. Children who need additional support are identified and supported during lessons. Our children are also encouraged to take part in richer Computing experiences, making links with local schools; international schools via our connecting classrooms project and with local colleges, businesses and universities where appropriate.

Teachers assess attainment regularly using assessment for learning strategies in class and using our online assessment platform. This allows for Teachers to identify necessary gaps and to plan to address these in future lessons.

Weston Mill Community Primary Academy –

Teaching and learning in Computing and E-safety at Weston Mill has taken place using an 'unplugged' approach – this has been an effective way of teaching computing skills in a whole class setting before consolidation using ICT equipment. As is consistent across the MAT, we follow two progression maps; one for Computing and one for E-safety, these builds on learning and skills taught each year, deepening the children's understanding across the subject and introducing them to new skills. The E-safety Progression Map is reviewed annually and is based on individual units shared by National Online Safety Platform linked with the UK Council for Internet Safety's 'Education for a Connected

World' 2020 framework. Computing units are planned using a cross curricular approach and is embedded within our themes complimenting the learning as well as standing alone. Planning at Weston Mill is driven through the STEM subjects. Children use STEM skills across all subjects and often use Computing at the end of a unit to draw conclusions, present findings or to share what they have learnt.

Each year we have focus on E-safety and our children develop an in depth knowledge of how to stay safe online. Utilising the MAT wide E-safety Progression Map (as outlined above), children engage in termly units. We have a dedicated safety week as well as posters in classrooms reminding children of how they can stay safe online. This links in nicely with much of our work in PSHE.

Computing is assessed in lessons using assessment for learning strategies and using our online assessment platform. This assessment allows teachers to focus on gaps in knowledge and also to track children's journey through the school's progression map.

Discovery MAT E-safety:

Across the whole trust, children engage in termly E-safety units focusing on a wide range of prevalent issues. The E-safety Progression Map is based on individual units shared by National Online Safety Platform linked with the UK Council for Internet Safety's 'Education for a Connected World' 2020 framework units and includes the following topics:

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

These lessons are planned and resourced using the MAT wide E-safety Progression Map developed in line with resources and units provided by the nationally recognised 'National Online Safety Platform'. Children from the Early Years Foundation Stage to Year 6 complete 8 units annually. Additional to this, children also take part in Safer Internet day and a Safety week as well as consolidating topics through their PSHE curriculum. E-safety is also embedded through our Computing curriculum where knowledge and skills are reinforced during each Computing unit.

Further information surrounding the Education for a Connected World 2020 framework can be found here: Education for a Connected World - GOV.UK (www.gov.uk)

Education – parents / carers

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

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

- Curriculum activities
- Letters, newsletters, website, VLE
- Parents and carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Frameworks developed to support children and parents: Education for a Connected World - GOV.UK (www.gov.uk)
- Reference to the relevant web sites / publications e.g. www.swgfl.org.ukwww.saferinternet.org.uk/http://www.childnet.com/parents-and-carers
- National Online Safety Platform:

Beechwood: http://nationalonlinesafety.com/enrol/beechwood-primary-school-pl6-6dx
Oakwood: http://nationalonlinesafety.com/enrol/oakwood-primary-academy-pl6-6qs
Weston Mill: http://nationalonlinesafety.com/enrol/weston-mill-community-primary-academy

National Online Safety Platform:

As part of our commitment to E-Safety, our MAT has access to the National Online Safety Platform. This online resource is shared with parents through a unique web address for each school. Parents are able to access a plethora of resources including Online certified CPD courses focusing on a range of E-safety topics; 'What parents need to know' guides which discuss a wide range of applications and programs available to themselves and their children. Additionally, they can access webinars which detail changes to government policy and provide further information about upcoming technological advances that both they and their children will experience. Each year staff engage in relevant and up-to-date accredited E-safety training and this is also available to parents via the platform.

Education – the wider community

The MAT will provide opportunities for local community groups and members of the community to gain from the MAT's E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- By ensuring that each academy website provides relevant E-Safety information for the wider community

- As is detailed for parents and carers, our wider community groups are able to access relevant E-Safety resources and applications through each schools National Online Safety Platform. This unique community platform provides a wide range of online training and resources.

Education & Training – staff and volunteers

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

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process. Currently, this CPD is delivered through our National Online Safety Platform where staff can access a wide range of relevant CPD linked closely with government policy, this training will also support each school within the MAT to achieve a yearly 'National Online Safety Certified School' Award.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the MAT E-Safety policy and Acceptable Use Agreements.
- The Computing Co-ordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Computing Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Board of Trustees

The Board will take part in E-Safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at or participation in training provided by a relevant organisation
- Participation in school training / information sessions for staff or parents/carers
- Online E-safety Training provided by National Online Safety Platform

5 TECHNICAL – NETWORK, EQUIPMENT, FILTERING AND MONITORING

5.1 Technical Infrastructure

The MAT will be responsible for ensuring that the MAT network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- MAT technical systems will be managed in ways that ensure that the MAT meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of MAT technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to MAT technical systems and devices.
- All users may be provided with Office 365 username/passwords that remains up to date within Domain: Discovery Mat's Active Directory. Users are responsible for the security of their username and password and must notify their teacher for any change of password.
- The "master / administrator" passwords for the MAT ICT system, used by the ICT Manager (or other persons) must also be available to the CEO or other nominated senior leader and kept in a secure place.
- The ICT technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes via RM Education.
- The MAT has provided enhanced / differentiated user-level filtering
- MAT ICT technical staff regularly monitor and record the activity of users on the MAT technical systems and users are made aware of this in the Acceptable Use Agreement.
- Users are to report any actual / potential technical incident / security breach to the ICT Manager and CEO as soon as possible.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the MAT systems and data. These are tested regularly. The MAT infrastructure and individual workstations are protected by up to date virus software and routine software updates.
- An agreed protocol is in place for the provision of temporary access of "guests" (e.g trainee teachers, supply teachers, visitors) onto the MAT systems.
- An agreed protocol is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted. All laptops and memory sticks to be bit-locked before being taken off site.

5.2 Systems configurations

- All internet traffic routed via RM for filtering and monitoring.
- All non-essential firewall ports are locked down to prevent intrusions.
- Teachers laptops are encrypted using Bit locker.
- Any equipment running End of Lifecycle software is removed from the network, only OS / iOS systems that are able to receive updates and service packs are supplied to students / staff.
- All equipment is installed with anti-virus and monitored.

- Students / staff receive individual accounts within a Hybrid environment linked with 365 Online.
- Students / staff computer equipment is managed by Group Policies implementing safe best practices and specific privacy settings.
- Students / staff data is stored on SharePoint and OneDrive enabling secure data storage, both platforms meet GDPR compliance.
- Remote Learning, Students / Teachers are locked under an automated script applying the Microsoft policy batch standards, Student Primary School Education for Remote Learning, and Teacher Primary School Education for Remote Learning. These policies are automatically applied to staff and students daily. Global configuration has been defined to force a lockdown default for the presenting of meetings to Organisers Only. Team creation has been locked to teachers only, preventing students from creating companywide Teams.

6 VISITORS/CONTRACTORS PROTOCOL FOR USING MOBILE DEVICES.

For visiting guests/contractors who require the use of their own devices to deliver presentations to members of staff or pupils or for general use must follow strict guidelines listed below.

- All Visitors/Contractors must be escorted at all times when using mobile devices.
- The MAT accepts no responsibility for lost or stolen items during their time within the MAT. Personal items must be kept safe at all times.
- Any information obtained during their visit that must not be shared to third parties and remain the sole ownership of the Trust.
- Whilst network systems are safe and secure, it is an offence for visitors to gain access to the Trust's Networks and will fall within the MAT's General Data Protection Policy.
- Visitors are required to keep their passwords safe and secure at all times.

7 USE OF PHOTOGRAPHIC IMAGES

Please consult the MAT's **Use of Photographic Images Policy**.

8 GENERAL DATA PROTECTION REGULATIONS

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The MAT will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a General Data Protection Policy in place (please see the MAT's **Freedom of Information and Data Protection Policy**)
- It is registered as a Data Controller for the purposes of the Data Protection Act (GDPR)
- Responsible persons are appointed - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with MAT policy once it has been transferred or its use is complete

9 COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the MAT currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

COMMUNICATION TECHNOLOGIES	times	ed staff			times	permission
Mobile phones may be brought to school	x					
Use of mobile phones in lessons						
Use of mobile phones in social time			x			
Taking photos on mobile phones / cameras /other devices			x			
Use of other mobile devices e.g tablets, gaming devices						
Use of personal email addresses in school, or on school network						
Use of school email for personal emails						
Use of messaging apps						
Use of social media						
Use of blogs						

When using communication technologies, the school considers the following as good practice:

- The official MAT email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the CEO – in accordance with the MAT policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the MAT website and only official email addresses should be used to identify members of staff.

SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

Please consult the MAT's Use of Social Media Policy.

UNSUITABLE / INAPPROPRIATE ACTIVITIES

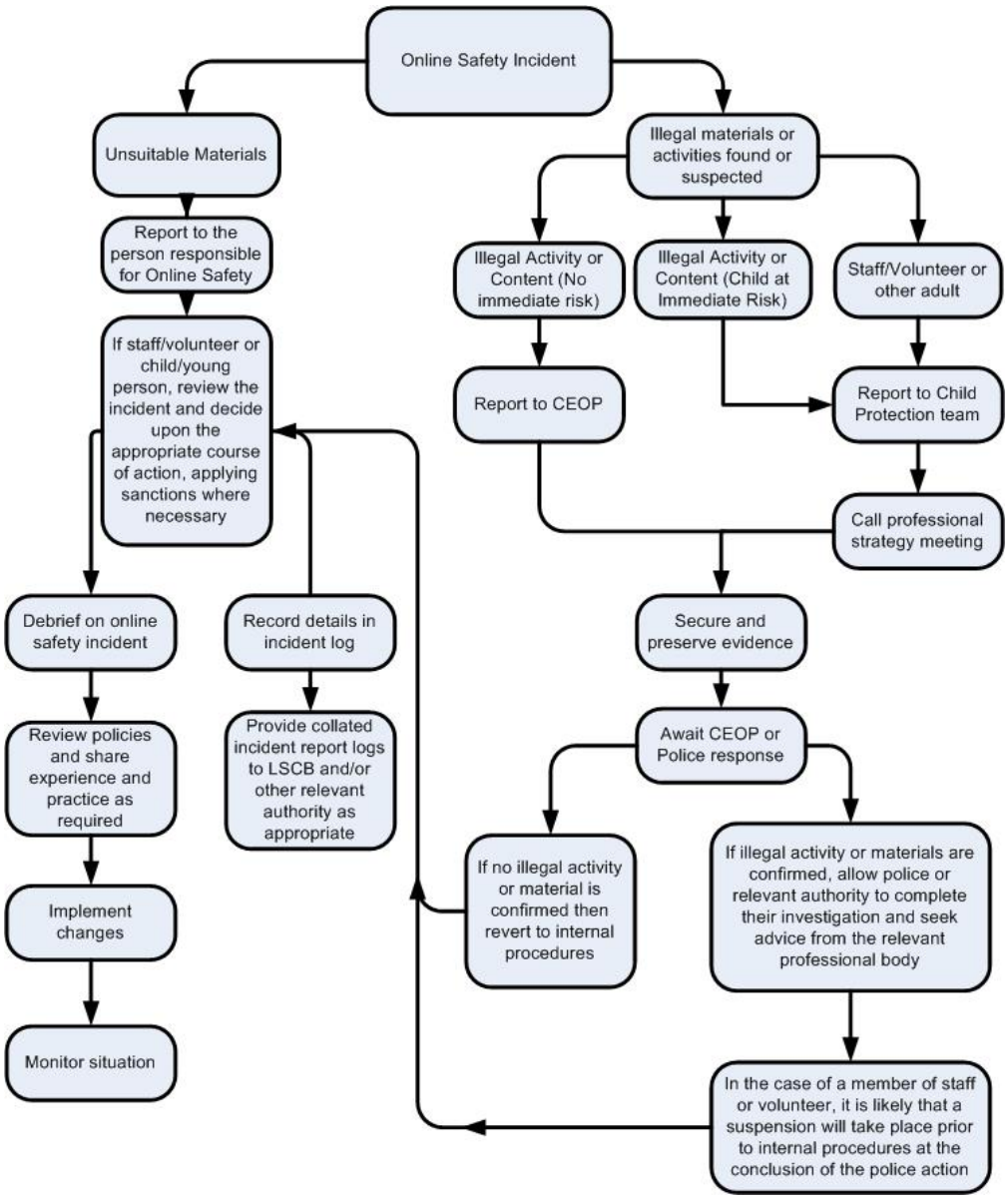
The MAT believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using MAT equipment or systems. The MAT policy restricts usage as follows:

USER ACTIONS		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography					X
	promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					X
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non-educational)					X	

On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting YouTube			X		

ILLEGAL INCIDENTS

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart overleaf before responding to online safety incidents and report immediately to the police.



OTHER INCIDENTS

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

MAT ACTIONS AND SANCTIONS

It is more likely that the MAT will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the MAT community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows. Please refer to the following MAT policies for further details: **Behaviour Policy, Disciplinary Policy & Procedures**.

STUDENTS / PUPILS **ACTIONS / SANCTIONS**

Incidents:	Refer to class teacher	CEO	Refer to Head of School	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X		X			X			

Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X			
Unauthorised use of social media / messaging apps / personal email	X		X			X		X	
Unauthorised downloading or uploading of files	X		X			X	X	X	
Allowing others to access school / academy network by sharing username and passwords	X		X		X	X		X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X		X		X	X		X	
Attempting to access or accessing the school / academy network, using the account of a member of staff			X		X	X	X	X	X
Corrupting or destroying the data of other users			X		X	X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X		X	X	X	X	X

STAFF

ACTIONS / SANCTIONS

Incidents:	CEO	Refer to Head of School	Refer to DPO	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X				Fol lo w Di sci		

Inappropriate personal use of the internet / social media / personal email	X	X				
Unauthorised downloading or uploading of files	X	X				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				
Deliberate actions to breach data protection or network security rules	X	X	X		X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			
Actions which could compromise the staff member's professional standing	X	X				
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X				
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		
Breaching copyright or licensing regulations	X	X			X	
Continued infringements of the above, following previous warnings or sanctions	X	X		X		

FURTHER INFORMATION

UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL& Diana Awards) - http://enable.eun.org/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - https://www.childnet.com/resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Data Protection

Information Commissioners Office:

https://ico.org.uk/

https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/?q=it+security

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Your rights to your information – Resources for Schools - ICO

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

Professional Standards / Staff Training

DfE- Safer Working Practice for Adults who Work with Children and Young People

UK Safer Internet Centre Professionals Online Safety Helpline

Education for a Connected World - GOV.UK (www.gov.uk)

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

National Online Safety Platform -

Beechwood: http://nationalonlinesafety.com/enrol/beechwood-primary-school-pl6-6dx

Oakwood: http://nationalonlinesafety.com/enrol/oakwood-primary-academy-pl6-6qs

Weston Mill: http://nationalonlinesafety.com/enrol/weston-mill-community-primary-academy

Education for a Connected World - GOV.UK (www.gov.uk)

Research

Ofcom – Children & Parents – media use and attitudes report – 2015

APPENDICES

APPENDIX A
STAFF ACCEPTABLE USE AGREEMENT

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

Discovery Multi Academy Trust ("the MAT") will endeavour to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff to agree to be responsible users.

ACCEPTABLE USE POLICY AGREEMENT

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

For my professional and personal safety:

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

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the MAT's Use of Photographic Images Policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on an academy website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the MAT's policies.
- I will only communicate with pupils and parents / carers using official MAT systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using MAT equipment. I will also follow any additional rules set by the MAT about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the MAT ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer
- I will not disable or cause any damage to MAT equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the MAT's Freedom of Information and General Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by MAT to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of MAT digital technology equipment in school, but also applies to my use of MAT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the MAT.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the MAT digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the MAT) within these guidelines.

Name: .....

Signed: .....

Date: .....

APPENDIX B

PUPIL ACCEPTABLE USE POLICY

FOR EYFS/KS1

A NOTE TO PARENTS AND CARERS

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. This E-Safety Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Discovery MAT will endeavour to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

PUPIL ACCEPTABLE USE AGREEMENT FOR EYFS/KS1

This is how I will stay safe when I use a computer:

I will ask a teacher if I want to use the computers.
I will only use activities that a teacher has told or allowed me to use.
I will take care of the computer and other equipment.
I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
I will tell a teacher if I see something that upsets me on the screen.
I know that if I break the rules I might not be allowed to use a computer.

PARENT / CARER SIGNATURE

As the parent / carer of the above pupil, I understand that the academy has discussed the Acceptable Use Agreement with my son / daughter as part of whole MAT commitment to e-Safety both in and out of school.

I understand that the MAT will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the MAT cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the academy if I have concerns over my child's e-Safety.

Name of Parent/Carer ……

Signed ……..

Date ……

PUPIL ACCEPTABLE USE POLICY

FOR KS2

A NOTE TO PARENTS AND CARERS

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. This E-Safety Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Discovery MAT will endeavour to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

PUPIL ACCEPTABLE USE AGREEMENT FOR KS2

These are the rules I agree to follow when using any digital technology:

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not use my mobile phone in school for any reason.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the Behaviour Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted.

I have read and understood these rules and agree to follow them.

Name of Pupil ……..

Class ……

Signed ……..

Date ……

PARENT / CARER COUNTERSIGNATURE

As the parent / carer of the pupil, know that my child has signed this Acceptable Use Agreement and has received, or will receive, E-Safety education to help them understand the importance of safe use of digital technology– both in and out of school.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the MAT cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

I understand that my child's activity on the ICT systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the academy if I have concerns over my child's E-Safety.

Name of Parent/Carer ……

Signed ……..

Date ……

APPENDIX C

COMMUNITY USERSACCEPTABLE USE AGREEMENT

This Acceptable Use Agreement is intended to ensure:

- that community users (for example, volunteers, supply staff) of MAT digital technologies will be responsible users and stay safe while using these systems and devices
- that MAT systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

ACCEPTABLE USE AGREEMENT

I understand that I must use MAT systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring onto MAT premises:

- I understand that my use of MAT systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into the academy for any activity that would be inappropriate in a school setting
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Head of School or other appropriate staff member
- I will not access, copy, remove or otherwise alter any other user's files, without permission
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the academy
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work

- I will not install or attempt to install programmes of any type on a MAT device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to MAT equipment, or the equipment belonging to others
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that if I fail to comply with this Acceptable Use Agreement, the MAT has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the MAT digital technology systems (both in and out of school hours) and my own devices (in school hours and when carrying out communications related to the MAT) within these guidelines.

Name: .....

Signed: .....

Date: .....