Colleague IT Acceptable Use IT Policy

The purpose of this policy to ensure that all devices and systems are used in line with expectations of the organisation with the aim to keep users and data safe and secure.

Version number	8
Consultation groups	Data Protection Officer, Director of People, Head of Safeguarding, Trust Leader.
Approved by	Paul Stone
Approval date	10/10/2024
Implementation date	10/10/2024
Policy/document owner	Director of IT
Status	Trust mandatory policy
Frequency of review	Annually
Next review date	September 2026
Applicable to	All colleagues, volunteers and SCITT students in all locations
Sources	

Document History

Version	Version Date	Author	Summary of Changes
V3	16th April 2018	Director of Operations	Revised Policy following GDPR
V4	30th March 2020	Head of Safeguarding	Revised due to COVID-19 changes to practice and working conditions / school closures / Remote Learning
V5	15th April 2022	Director of IT	Branding update, adding in an example of a password manager.
V6	9th May 2023	Data Protection Officer	Condensed GDPR statement for better understanding and added info about GDPR Sentry. Statement added about email retention policy.
V7	29th June 2024	Director of IT	Added point on connecting to BYOD wireless network.
V8	10th October 2024	Director of IT Director of People Head of Safeguarding Data Protection Officer	- Updated initial sentence - Updated email retention period. - Added additional users to the scope. - Added about use of MFA. - Updated staff/pupil to colleague/child. - Added AI statement

1. Purpose

Technology is now entwined in our modern lives with everyday use of social media and web-based communication a standard practice. It is therefore important to ensure good awareness both of the possibilities to learn, create and share ideas and also the risks that these freedoms bring both to the welfare of colleagues and students and to the integrity of the ICT systems that the school relies on to provide learning and teaching.

All users accessing our school systems are entitled to safe access to the internet and IT systems at all times. This policy is intended to provide a working framework for colleagues to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

This is not an exhaustive list, and all colleagues are reminded that ICT use should be consistent with the organisations ethos, GDPR regulations, other appropriate policies, relevant national and local guidance and expectations, and the Law.

2. Scope

The policy applies to:

- All Discovery colleagues, volunteers and SCITT trainees.
- Information assets, whatever format, device or medium they are held in.
- All Discovery owned information, in whatever format, wherever it is held (e.g. by a third party) for which Discovery is the data controller.

3. Your Responsibilities

3.1 I understand that Information Systems and ICT include networks, data, and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email, and social media sites.

3.2 Discovery Schools Academy Trust Ltd owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3.3 I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will not transfer organisational data to personal devices.

3.4 I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password (following organisation policies) and will not store

this password in an insecure location. Where possible I will always use Multi Factor authentication as an additional security measure. It is recommended that you use a password manager such as Enpass.

3.5 I will not attempt to install any purchased or downloaded software or hardware without permission from your line manager and the IT Department.

3.6 I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place. Any data which is being removed from the school site's (such as email) will be encrypted by a method approved by the IT Department. Any images or videos of pupils will only be used in line with organisational policy and will always consider parental consent before processing. All organisational data must stay on organisation owned devices and never be transferred to personal devices.

3.7 I will not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access the organisations email system on my mobile device (tablet or mobile phone), the device must be pin, or password protected. I will protect the devices in my care from unapproved access or theft. We block access to organisation data from outside of the UK by default and only in some circumstances shall this be allowed. Please contact the IT Service for information on the approval process.

3.8 Personal data kept on work devices must be kept to a minimum (examples that **do not** meet this include filling the hard drive with music files or personal photos). I will ensure that I regularly cleanse data from my device/OneDrive to reduce unnecessary storage.

3.9 I will respect copyright and intellectual property rights including but not limited to the use of copyrighted images.

3.10 I have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3.11 I have carried out Data Protection and GDPR training via appropriate trust CPD programmes, i.e., Flick Training, Sentry

3.12 I have read and understood the Discovery Mobile Phone and Loaned Property Equipment policy that covers the use of any phone/loaned equipment that I may have been provided to carry out my work.

3.13 I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (DSL) and line manager as soon as possible. I will report any accidental

access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and your line manager.

3.14 I will not attempt to bypass any filtering and/or security systems put in place by the organisation. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Department as soon as possible.

3.15 I will report any actual or potential data breaches to the Local Data Protection Representatives (or DPO if central team) within 24 hours of the incident. The LDPR will upload data breaches to our GDPR System (GDPR Sentry).

3.16 I understand that Office 365 mailboxes (email) are not a storage system, and that the organisation has a policy in place to delete emails after 3 years. Emails that are required beyond this put need to be saved outside of mailboxes.

3.17 My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will always be transparent and open to scrutiny. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.

3.18 I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes, but not limited to, the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the organisations AUP and the Law.

3.19 I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the organisation I work for into disrepute.

3.20 I will promote online safety and will help colleagues and children to develop a responsible attitude to safety online, system use and to the content they access or create.

3.21 I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on all colleague's member's devices.

3.22 Any personal device will only ever be connected to the BYOD wireless network communicated by the IT team.

3.23 I understand that the use of USB storage devices is prohibited and agree not to use them.

Use of live webcams and online chat software for use in remote teaching and learning

3.24 I understand that no 1:1 conference calls or chats will be used, either colleague to child or child to child, and that groups of children only will be organised by the teacher / adult leading the session.

3.25 I understand that colleagues and children must wear suitable clothing (no PJ's or offensive slogan T-shirts), as should anyone else in the household when webcams are switched on. It will be the adult's responsibility to immediately switch off any webcams or remove from the group a child's account, if they felt a child or family members clothing was inappropriate.

3.26 I understand that any devices used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background (to avoid the endorsement of use of consumer products). It will be the adult's responsibility to immediately switch off any webcams or remove from the group a pupils account, if they felt the room being seen was inappropriate. The blurring of backgrounds tool will where possible will always be used.

3.27 I understand that it is my responsibility to ensure that the live class is recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed. Any safeguarding concerns seen or heard will be recorded on CPOMS and reported to a DSL immediately.

3.28 I understand that live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day. The time-of-day live classes are timetabled will always fall within normal school hours.

3.29 I understand that my language must be professional and appropriate, including any family members/adults in the background of my household. Inappropriate language used by pupils or heard by members of their family will be challenged and accounts will be muted, if necessary, by the adult.

3.30 I understand that Webcams and chat platforms are for work purposes only and subject to the code of conduct standards set out in the organisations staff behaviour policy. A breach of these standards may result in disciplinary action.

3.31 I will risk assess any AI platform before entering any colleague/student personal data. I will ensure that I respect age limit guidance when using generative AI tools. I.e., Copilot age limit guidance is 16.

I understand this forms part of the terms and conditions set out in my contract of employment and failure to adhere may result in disciplinary action.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.	
Signed:	
Print Name:	
Date:	