Building resilience not reliance.

GANTON SCHOOL

Acceptable Use Policy

We are a Rights Respecting School in accordance with UNICEF (United Nations Children's Fund). Our aim is to promote and protect the rights of all children in Ganton School to an education, to be healthy, to have a childhood, to be treated fairly and to be heard so that they can survive, grow, participate and fulfil their potential. Ganton School puts the United Nations Convention on the Rights of the Child (CRC) at the heart of all policies, practice and ethos.

Everyone at Ganton School who comes into contact with children and families has a role to play in safeguarding and promoting the welfare of children by;

- protecting children from maltreatment
- preventing impairment of children's health or development
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- taking action to enable all children to have the best outcomes.
-

Working Together to Safeguard Children 2015

Headteacher: Mr Eddy Wharton

Review Date: January 2024

An inclusive community committed to excellence in personalised learning and well–being.

HumberEducationTrust

Ganton School
Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Ganton School's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Ganton School's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that Ganton School's systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

This Policy should be read in conjunction with the school's E-Safety and Mobile Devices Policies.

Introduction

As part of Humber Education Trust's programme to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), it has a suite of Information Governance policies available through Veritau.

The Acceptable Use policy governs the use of the school's corporate network that individuals use on a daily basis in order to carry out business functions.

This policy should be read in conjunction with the other policies in Veritau's Information Governance policy framework.

Scope

All policies in Veritau's Information Governance policy framework apply to all Humber Education Trust school employees, any authorised agents working on behalf of the school, including temporary or agency employees, and third-party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

EMAIL AND TEAMS CHAT USE

The school provides email accounts to employees to assist with performance of their duties. The school also allows employees to use its instant messaging service via Teams Chat. For the benefit of doubt instant messages are classed as email communications in this policy.

Personal Use

Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the school,
- Employees understand that emails sent to and from corporate accounts are the property of the school,
- Employees understand that school management may have access to their email account and any personal messages contained within,
- Employees understand that the emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the school reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use

The school does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary,
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use

Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Email Security

Users will take care to use their email accounts in accordance with the school's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the school's IT network,
- Not send excessively large email attachments without authorisation from school management and the school's IT provider.

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. The Headteacher / Chief Operating Officer will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The school may monitor and review all email traffic that comes to and from individual and group email accounts.

INTERNET USE

The school provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the school,
- Employees understand that school management may have access to their internet browsers and browsing history contained within,
- Employees understand that the school reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The school does not permit individuals to use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Internet Security

Users will take care to use the internet in accordance with the school’s information security policy. In particular users will not click on links on un-trusted or unverified web pages.

SOCIAL MEDIA USE

The school recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The school also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts

The Trust has a number of social media accounts across multiple platforms. Nominated employees will have access to these accounts and are permitted to post general information about the school. Authorised employees will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. The Headteacher / Chief Operating Officer will have overall responsibility for allowing access to social media accounts.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the school's information governance policies and data protection legislation.

Corporate social media accounts must not be used in a way which could:

- Tarnish the reputation of the school,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit,
- Be construed as political beliefs or commentary.

Personal Accounts

The school understands that many employees will use or have access to personal social media accounts. Employees must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach clients, customers, or partners of the school.

TELEPHONE AND TEAMS USE

The school provides email accounts to employees to assist with performance of their duties. The school also allows employees to use Teams for business. For the benefit of doubt Teams calls are classed as telephone calls in this policy.

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the school,
- Employees understand that school management may have access to call history,
- Employees understand that the school reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions.

Inappropriate Use

The school does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Telephone Conduct

Employees are expected to conduct themselves in a professional manner whilst using the telephone.

I have read, understood and agree with the ICT Acceptable Use Policy in relation to information systems.

Print Name: ______________________________________

Signed: ____________________________________

Date: ____________________________________

Please sign and return this page to the School Business Manager. A copy of this agreement will be retained on the employee's personnel file.

Appendix 1 – ICT Acceptable Use Policy – New Starter Login Details

HumberEducationTrust

IN STRICT CONFIDENCE

New starter computer log-in for:

Name: ____

Role: ____

Start Date: ____

Your email address is: ____

Please use the username and password below to access emails and one drive via SharePoint https://hetacademy.sharepoint.com/

Username	
Password	

Please use the username and password below for your Computer login:

Username	
Password	

Please use the username and password below in ScholarPack:

Username	
Password	

Please use the username and password below in CPOMS:

Username	
Password	

Once you have logged in you will be asked to change your password.

Never give your username and password to anyone else.

Please note: The use of these log-in details will confirm your acceptance of the ICT Acceptable Use Policy

Appendix 2 – ICT Acceptable Use Policy – Do’s and Don’ts

Dos and Don’ts of Data Protection for School Employees

Password Security

Do…

- Keep your password safe
- Change it frequently
- Make your password very hard to guess - Include a mix of upper and lower case letters, numbers and punctuation marks

General Security

Don’t…

- [illegible]

Do…

- Lock your laptop if you are away from your workstation using ‘ctrl+alt+delete’
- Keep paper files containing personal information locked securely
- Use the ‘blind copy’ function when appropriate

Don’t…

- Leave personal or special category information out overnight or if you are away from your workstation

Data Breaches

Remember- serious data breaches must be reported to the Information Commissioner’s Office (ICO) within 72 hours

Do…

- Have a procedure in place to ensure staff are aware of how to report an incident
- Report any incidents to the appropriate member of staff straight away
- Report any serious incidents to your Data Protection Officer

Sending Special Category Data

Details about

Do…

- Take extra care when sending special category information externally
- Send emails containing sensitive information securely (e.g., Egress)
- Post information securely
- Ensure contact details for your data subjects are ACCURATE AND UP TO DATE

- Sex Life
- Race/Ethnicity
- Religion/Philosophy
- Mental or Physical Health
- Political Views
- Trade Union Membership
- Criminal History
- Biometrics (Thumbprints)
- Genetics

Retention and Disposal of Records

Do…

- Maintain a retention and disposal schedule
- Ensure that electronic systems have the capability to delete information
- Ensure printers that store data are being properly cleansed before being returned

Don't…

- Hold information 'just in case' (make sure you comply with statutory retention periods or have an organisational need to retain the information)
- Dispose of personal or special category information carelessly – paper files will need to be shredded and electronic information must be permanently deleted

Working from Home

Do…

- Ensure you follow your school's policy that sets out expectations for home working
- Keep information in a secure place within your home
- Only use authorised 'cloud products' for personal data
- Only use encrypted memory sticks of personal data

Don't…

- Email work to your personal account or download personal information to your own laptop
- Allow family or friends to have access to this information
- Leave paper files or devices in your car overnight

Subject Access Requests (SARs)

Do…

- Remember that SARs can be made verbally under the UK GDPR
- Comply with requests within 30 calendar days (unless an extension of up to 2 months is appropriate)
- Ensure that you can easily retrieve information and know where it is located
- Follow your internal policy and procedures for answering requests.

Don't…

- Withhold information from a SAR unless an appropriate exemption applies

Remember- anything you record in writing about an individual has the potential to be disclosed under subject access!

Data Subject Rights

Do…

- Remember your pupils and parents have strong rights over their personal information including:
  - Right of access (SAR)
  - Right to be informed
  - Right to rectification
  - Right to object
  - Right to erasure

- Ensure your data subjects know they can complain to the DPO if they have a concern over how you are handling their data

Contracts Management

Do…

- Ensure a contract is in place between the School and any 'Data Processors'
- Ensure all contracts have 'Data Protection Clauses' within,
- All contractors are listed on a contracts register,

Initial Equality Impact Assessment

Impact Groups	Pupils	Staff	Families	Governors	Volunteers	Visitors	Wider Community
	✓	✓	✓	✓	✓	✓	✓

Does or could this policy have a negative impact on any of the following?

Age			Disability			Gender			Gender Identity			Pregnancy or Maternity			Race			Religion or Belief			Sexual Orientation			Verdict	
Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N
	✓			✓			✓			✓			✓			✓			✓			✓			✓

Does or could this policy help to promote equality for any of the following?

Age			Disability			Gender			Gender Identity			Pregnancy or Maternity			Race			Religion or Belief			Sexual Orientation			Verdict	
Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N
✓			✓			✓			✓			✓			✓			✓			✓			✓	

Does data collected from the equality groups have a positive impact on this policy?

Age			Disability			Gender			Gender Identity			Pregnancy or Maternity			Race			Religion or Belief			Sexual Orientation			Verdict	
Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N	?	Y	N
✓			✓			✓			✓			✓			✓			✓			✓			✓	

Conclusion:	We have come to the conclusion after taking an initial equality impact assessment that a full assessment is / **is not required.**	
Status of Policy:	Existing Policy	
	New/Proposed Policy	✓
	Updated Policy	

Initial Equality Impact Assessment completed by:
Sue Jones

Initial Equality Impact Assessment approved by:
Senior Leadership Team

Date: 24/4/16